Blacklisted! 411

The official hackers magazine

HACK THE SYSTEM...

The Art of Casual WiFi Hacking

A hands-on look at wardriving.

Also inside this issue:

- Hacking the Mirra M-250
- Auditor: Debian WiFi Hacking
- Cheating on Browser-based Games

VOLUME 7 ISSUE 4 FALL 2005

Blacklisted! 411 v7i4
$5.95 U.S. $7.75 CAN

This publication is dedicated to all of those before us who built the foundation for the hackers of the world to express themselves openly and without prejudice.

While we attempt to continue in our quest to obtain knowledge and understanding, we invite you, the reader, to join in and share any thoughts you may have regarding the magazine, hacking, life, work and anything else that you feel is important enough to be shared.

We're not going to knock anyone down for asking questions or ridicule the steadfast elitist folks who believe that knowledge should not be shared. We believe knowledge should in fact be shared with one another, no matter how trivial the information may appear to be. After all, knowledge is power.

Think back to the way it was, when hackers stuck together and had a good time. An amusing time when hackers shared their stories of exploration and ultimate conquest. A wondrous time when hackers were considered the good guys and looked up to by those not fortunate enough to understand the technology around them. A simple time when a hackers harmless efforts gained a new understanding of technology issues and the praise from their peers and superiors alike.

That time can still be NOW. Hackers of the world unite and exercise your freedom to disseminate information!

Blacklisted! 411 staff & contributors

Editor in Chief
Zachary Blackstone

Assistant Editors
Alexander Tolstoy
Dave S.

Office Help
Pixel Pixie, Jess, Lexus, Dark Paladin, DoctorWHO, MomoPi, Mr. Asshole

Artwork
Derek Chatwood - A.K.A. Searcher
Kate O., Parallax, Mason/Wolf

Distribution
Greg, Boiler, Syntax, David B.

Photography
CHS, Dark Paladin, Daniel Spisak

Forum Admin
*Ustler_*

Writers
ML Shannon, Ustler, Unicoder, Dr. Fibes, Jeremy Martin, The Goldfinger, Dual Parallel, MobbyG, Cactus Jack, Israel Torres, Grandpa Hackman, Electra-Solve

ISSN 1082-2216

Blacklisted! 411 Magazine
P.O. Box 2506
Cypress CA, 90630

9035768ABBAJBVJB-0024

DBBL 01,07,32,41,52

PRINTED IN THE UNITED STATES OF AMERICA

Blacklisted! 411 shout outs

Doc Salvage
ECSC
oleBuzzard
Dark Tangent
DEFCON
Freaky
Blackwave
IrvineUnderground
Consumertronics
Wizguru
Greyhawk
*Spratt_*
The Underground Mac
Bobeeve
German
Big Dog
Skippy
Avatar
Neuromancer
Doc Jones
LineTech
Alaric
Short Circuit
Mingle
The Goldfinger
E. Coli
Group 42
SWAT
Trash-OOX
Doule-O-Jake
Ender Wiggin
TechnoHeap
GI Electronics
Lucky225

....and a few ANONYMOUS people

Inside this issue

Additional information

How to Contact us:
Blacklisted! 411 Magazine
P.O. Box 2506
Cypress, CA 90630

Subscriptions:
$20 U.S., $24 Canada, $35 Foreign
Check or Money Order (U.S. Funds only)

Articles:
Blacklisted! 411 Articles
P.O. Box 2506, Cypress, CA 90630
(Include name & address—we PAY for articles)

Letters:
Blacklisted! 411 Letters
P.O. Box 2506, Cypress, CA 90630

Distribution and Sales:
Blacklisted! 411 Distribution
P.O. Box 2506, Cypress, CA 90630
Email: sales@blacklisted411.net

Advertising:
Blacklisted! 411 Advertising
P.O. Box 2506, Cypress, CA 90630
Email: advertising@blacklisted411.net

World Wide Web:

Website: **http://www.blacklisted411.net**
Store: **http://store.blacklisted411.net**
Forums: **http://www.bl411forums.com**

Blacklisted! 411 introduction for those of you who are new…..

Who we are… and were…

The question often arises on the subject of, "How did it all start?" in reference to our magazine and it's history. In response to this popular question, here is a quick history lesson of *Blacklisted! 411* magazine, including names, dates and little known facts which have, thus far, been hidden away for years…

Blacklisted 411 magazine dates back to October 1983 with a group of friends from a Southern California high school that shared a common interest. They were all deeply interested in their Atari, Apple and Commodore computers, electronics, sciences, arcade games, etc. They built projects, hacked into various things, made their own programs, came up with grand ideas and tried to make them into some sort of reality. The group started a monthly hackers "disk magazine" (an early form of what is now known as an e-zine) called "*Blacklisted 411, the hackers monthly*". This may sound strange today but circulating information on disk was the best way to get it out (at the time) without all the cool toys we take for granted today. There was no internet to utilize and nobody had printers which could print anything other than plain text (and didn't even do that well). With a disk based system, text files, primitive graphics/ pictures, and utilities were fairly easy to distribute and it could be copied by anyone who had a compatible computer. At the peak, at least 150 disk copies <per month> of the disk magazine we sent into the world, though there is no way to know how many were copied by others.

Eventually modems caught on and the magazine was distributed through crude BBS systems. Using the power of a Commodore 64, a *Blacklisted! 411* info site, which anyone could log into without handle or password, was created and operated. It was a completely open message center. Using X-modem or Punter file transfer protocols, one could download the latest *Blacklisted! 411* files or read/leave "messages" which later became known as a "message base" and has evolved into what are now commonly known as "newsgroup postings" or "forum postings". There was only one message center, no email capability & only 1 phone line. Primitive, indeed. Effective, however.

Around 1984, the purchase of a 9 pin dot matrix printer that could <gasp> print basic graphics was entered into the mix. Printing out copies of the *Blacklisted 411 monthly* and copying them at the media center at the high school became the new "experiment". The media center staff graciously allowed the production of these copies free of charge which was very cool at the time. The copies were passed out at the local "copy meets" (an interesting phenomenon of past times - hordes of computer users would meet at a predetermined location and setup their computers with the sole purpose of copying software and exchanging this software with each other). Piles of the magazine were left anywhere and everywhere people could see them. One popular location was next to the Atari Gauntlet and Gauntlet II arcade games strategically located at 7-11's all over the place. It's been a longtime myth that people photocopied those original copies and then those were photocopied, etc. There's no telling just how many generations of early printouts of *Blacklisted! 411 monthly* made it out there.

Years went by and *Blacklisted! 411* evolved. The short life-span of the printouts was both a great success and a miserable failure. No matter where they were left, they were taken - and taken quickly! The feedback was awesome in that people wanted more. The interest was very high, but the inability to meet this growing demand was completely overlooked. The plug was officially pulled on the printout experiment and distribution through diskettes remained the norm. It was really the easiest way to go at the time. The *Blacklisted! 411* info site grew into a 2-line system. This was a big deal in 1985. By that time, information was almost exclusively passed around by modem (unofficially on paper) and disks were still being released at this time.

June of 1987 marked the end of *Blacklisted! 411, the hackers monthly*. The last disk based magazine (# 46) was distributed that month. Since all of us original crew were finally out of high school and onto college, work and the bigger/better things in life, nobody had the time or inclination to put any effort into the disk based magazine anymore. The once thriving *Blacklisted! 411* group broke up and people went their separate ways. Naturally, it was assumed that this was the end and *Blacklisted! 411* would never be resurrected in any form.

In the summer of 1993, one member (and the original editor-in-chief), Zachary Blackstone, felt it was time to revive the *Blacklisted! 411* concept, but this time do it as a print magazine. It was extremely difficult to get started because the group was no more and he was alone. He was the only one of the original group members remaining that had an interest in bringing the hacker group and magazine alive again. With some money, the will to make it happen, top of the line (at the time) computer gear and page layout software, *Blacklisted! 411* was reborn. *Blacklisted! 411* Volume 1, Issue 1 was released in January 1994. *Blacklisted! 411* was finally BACK. The issues were released monthly and distribution was small. Regardless, the related user meets were packed! The interest in the magazine was great. After a year passed, it was decided to try a quarterly format in an effort to increase distribution. During that year Zachary managed to get in contact with many of the old group members, most of whom which are active staff members even today.

In 1999, what was to be the last issue of *Blacklisted! 411* (Volume 5, Issue 4) was published. It was unknown at the time, but many pitfalls would ultimately cause the demise of the magazine. Officially, it was dead as a doornail. After 4 years of regrouping and planning, *Blacklisted! 411* magazine was resurrected yet again..

To date, Blacklisted! 411 is one of the oldest group of hackers still remaining and releasing gathered and compiled information within the hacker community and the mainstream community as well. Hanging onto the very same hacker mentality and code of ethics from the 80's, Blacklisted! 411 stands apart from the rest. Their ideal is that hackers are not thieves - they're curious people who are the makers and shakers of the technology sector. They're not elitist hackers by any means and believe that no question is ever a "stupid" question. Old school hackers and newbie hackers alike, Blacklisted! 411 caters to you.

What' about now…

Community

Over the last year and a half, a lot has been happening. We have become more active in the Hacker Community. As we are based in the Los Angeles area, we have built relationships with the local Hacker groups such as LA2600, SD2600, twentythreedotorg, Irvine Underground and more. We have been attending and sponsoring Hacker Conventions and Conferences such as the Layer One Convention and the ever popular Defcon. You can find us attending these conventions regularly. We usually have a booth at these events where we sell subscriptions, current and back issues of the magazine, and other swag. We also provide several "convention only" promotions so look for us there.

Magazine Development

A major effort is being made to increase our exposure to the Hacking and Information Security Community. Our distribution goals for the magazine was to break 100K copies distributed each quarter sometime in 2004 and we surpassed our goal within our timeframe.. Based on orders from distributors and sell through, nobody comes even close to touching us in the hacking arena. We have been seeking and hiring freelance writers, photographers, and editors to increase the quality and scope of the magazine. Additionally, we have people who are actively trying to promote the magazine both inside and outside of our close community.

Merchandising / SWAG

We now have a whole series of *Blacklisted! 411* themed swag and merchandise. This currently includes stickers and apparel, but will soon include posters, a new DVD and whatever else our creative minds can come up with. Input, help, and direct submissions for this will be accepted and appreciated.

Charities

Blacklisted! 411 is run by real people who care about other things aside from hacking. No, really. In the spirit of helping people and organizations outside of our community, *Blacklisted! 411* Magazine has officially donated to the local chapter of the Ronald McDonald House charity. After all, children are our future. *Blacklisted! 411* Magazine wholeheartedly supports the Ronald McDonald House mission and their programs. Additionally, we've donated heavily to the Westminster Parish Festival, specifically with the intent to help support their youth programs and special classes for the mentally and physically handicapped.

If you have questions, comments, articles, ideas, flames, general "screw you guyz" messages or wish to offer support in some way, please contact us immediately and let's see what we can do. Thanks for your support, hackers!

BL411

Letter from Zachary Blackstone, editor-in-chief…..

Welcome to the newest edition of Blacklisted! 411 magazine, the official hackers magazine. A lot has been going on since the Summer issue first appeared at Defcon 13 this year. We were finally able to come up with SWAG to give away (and sell to some small degree). The shirts seem to have been a hit, while the hats were received with mild attention. The sixteen various bumper sticker designs were also a hit, we've actually seen them on cars throughout the SoCal area from time to time. That's pretty cool to see them in use.

Ok, I've got a lot of ground to cover and only one page to cram it into, so let's get started.

I'm going to mention a little bit about Defcon this year. Overall, we believe the event was an incredible success, both for the staff and owners of the event itself, but also for the visitors and our booth. Everyone had a great time and walked away knowing there's simply no better hacker convention on the planet! No doubt, if you visited our booth, you met our "booth babes" who were handing out free copies of the Summer issue. They were a new addition to our booth operation and we think they did a great job this year. Thanks girls! Everyone seemed pleased to receive free copies of the Summer issue, too. It's a small gesture we make to the community each year at the conventions we attend. It's not much, but it's the thought that counts, right? We also held a small raffle and gave away free swag, subscriptions and even a few 20GB Apple IPOD's. When it's all said and done, we had an awesome time at Defcon this year. So, with that said, count on seeing us there next year!

Something new that I'm really excited about is the fact that our magazine has gone from a 60 page format to an 84 page format, bringing this little zine to the top position as far as page count goes. That's right, we just added 24 more pages of content per issue! We've been getting so much support from the community lately, we decided it was time to add a few more pages, filled with hacking content. You'd think that we'd have to pass the extra cost onto our readers, but that's not true. The price of the magazine has NOT been increased because of this change. We sincerely hope that you enjoy the additional page count and the added content.

Big news on the hacker radar is our website. Yes, many of you are already aware of this, but we recently upgraded our website. When I say "upgraded" it doesn't even begin to tell the story. The old look was getting tired and didn't really appeal to anyone, including myself. So, in a combined effort, we made sweeping changes to the website, including the addition of new content in the form of articles and reviews, and massive expansion of already existing material. We even added new sections, complete with cover scans (from volume 1 all the way through volume 7), table of contents, sample articles and a little text about what was going on at the time of publication for each issue. There's some really interesting stuff to read and look at.

The new look is simply stunning, considering the rundown look of the site beforehand. If you have not seen it yet, you really must visit our website and check it out right away. In case you forgot, the URL of our website is www.blacklisted411.net

Something new which is sweeping the hacker community is our new monthly "online edition" of Blacklisted 411 which we've called "Blacklisted 411 .NET" Introduced in the middle of October, it's already taken off to an incredible start. It's a little something we cooked up to try and give back to the community. Many people have asked if the online edition would be an electronic version of the print magazine. The answer to this question is a resounding NO. The online edition is completely separate of the print version and contains articles and other material which is entirely different from the print version of our magazine. The only thing similar is the name. Anyhow, since the recent news of Phrack going out of business, we decided to try and pick up some of the slack and offer a FREE online hacker magazine. We're not trying to replace them, just give the hacker community something they don't have to pay for. Available as a PDF, we'll pump out a new issue each month, so visit our website often and make sure to grab your copy. Remember, it's absolutely FREE and you're welcome to copy it, upload it, mirror it, P2P it, archive it, print it, pass it around to your friends, etc. All we ask is that you give us credit and a link (www.blacklisted411.net) if you use any of the material for any purpose.

Well, that about sums up all the new stuff going on right now. Naturally, we're always on the lookout for new talent in the form of writers, artists, photographers and anyone else who can add to the value of our magazine. Among other things, one of the main reasons that we're set apart from other hacker magazines is that we actually PAY our writers, artists and content providers. Information may want to be free, but in reality, GOOD information usually has to be paid for.

Additionally, we're looking for active individuals who will POST in our forums. Having an active and fun forum area takes the effort of many people. We've provided the "arena" now it's time you kick yourself in the rear end and get posting.

We're a magazine, produced by hackers and made for hackers. We believe in being a team player and welcome everyone to voice their opinions. Hack the System!

- Editor

Notes of interest:

- T-shirts, baseball caps and bumper stickers are now available on our online store.
- Deadline on all articles, letters, artwork and ads for Volume 8, Issue 1 is January 13th, 2006.
- ALL classified ads are now FREE and are limited to space constraints per issue. First come, first served.
- We're a PAYING MARKET for articles we use! We pay $25-$450 depending on size, quality & use of photos.

Hi Zach, I am a new subber and am looking forward to getting Blacklisted 411 in the mail. The little paragraph that is on the first page of the mag is what really got me to subscribe. The forum seems to be a little slow . I'm not a computer hacker and don't really know anything about them. I am still in the physical world and cyberspace is a bit hard for me to grasp so I get along better with stuff I can touch and rewire and modify with a soldering iron. I love electronic gadgets and instruments. I hope I can find common ground with a few of the hackers here and maybe even learn something. I wish I could be as fortunate to be in an area where people are actually willing to come to gather at a place of regularity. I am in the middle of nowhere and you just cannot get people out here to get together for anything. We have tried to start a ham radio club several times and no dice! Of course my niche is any kind of radio and I love metal detecting. So thank you for having the wireless listing on the forum. It sounds like you have a fun group there at Blacklisted 411 and always savor the experience of commoradarie because it is getting harder to find good friends. So Zach thank you for the mag and taking me on board. Take it easy and CU later Zach. Nice meeting you.

Wirechief

Hey Wirechief. Welcome aboard! Glad to have you around. I can completely understand where you're coming from. My background was in electronics before I ever touched a computer—my first computer was an Altair that I built myself in the 70's. Having built my first computer at a component level, I was easily sucked into computers, making the jump from electronics to computers quite simple for me. Anyhow, in the spirit of "old school hacking" I intend to make available some small electronic projects related to hacking in some way. If all goes as planned, we'll even be able to provide circuit boards and part kits, just like the old electronic magazines used to do. I think that might go over well with people like yourself who want to get hands-on time with their soldering iron and other tools. Keep watching, we're bound to get some of these projects in an upcoming issue of Blacklisted. Maybe even this issue.

So, the point is that if you have a love for electronics, you've already got common ground with most hackers right off the bat. Let me tell you, the staff over here at Blacklisted! 411 love their electronic gadgets to no end. We always have some new toy to play with. You're in good company.

As for the forums, unfortunately they are a little slow. It takes the effort of many to keep the forums active, even in the face of apparent inactivity. It's something we intend to "work on" as time goes on. Keep posting in the meantime.

I've only just come across your magazine and I'm wondering if there is any place in the UK that may sell your magazine, we have nothing like this here. Thanks

Iceman

Hi Iceman. Blacklisted! 411 magazine is available throughout the United States, Canada, Mexico, Ireland, Japan, Israel, Hong Kong and various other destinations across the globe. Particularly in the U.K., our title used to be available at Tower Records in your area, but they pulled out of the area recently during a "rearrangement" of their company. To date, I'm not certain that our magazine is available at any location within the U.K. We don't have a complete listing of our availability at this time, so I can't give you 100% accuracy on exact locations where our magazine is or isn't being sold at the time, but it appears from an initial look that we do not have any distribution into the U.K. for the time being. I could be mistaken, however. I will research this further and see if we can correct this serious gap within our distribution chain.

To Any Personnel at 2600 Magazine or Blacklisted 411 Magazine who might be able to Help:

I've been trying. I've been trying really hard, but it just never seems to work. I don't know whether it's just pure bad luck, my own inherit stupidity, or any combination thereof that might be the deciding factor, but for some reason, the shit just doesn't work.

I'd like to call myself a hacker. I really would, but the closest thing I've ever come to "hacking" was vandalizing one computer back in my first High School programming class... and that wasn't even that difficult. It's been five years since then, and I don't think that I've gotten very far in my endeavors. It may be that I don't have enough time to commit to the art itself, or that, perhaps, I'm simply not able to hack, but I want to. You have no idea how badly I want to, either. Badly enough to spend hours up ever night sifting through bullshit website after bullshit website, trying to find the one bit of information I needed, the one text file I overlooked that may hold the key between gaining access to systems, and my unfortunate and woeful lack thereof.

I turned to my friends who claimed to be hackers. All I found there was senseless bullshit wrapped in a tasty Gothic shell. I tried searching the internet for programs that might have been what I was looking for, only to cast them aside after being called a "script kiddie." Elitist hackers in their far-superior mentality...why can't they see that I'm not some wannabe, but that I truly Want To Be? Why can't they remember that, at some point, at least one of them was just like me--searching for answers down the alleys of Digital Infinity.

I have no clue where to begin. I'm on a 56K modem, running AOL. For the moment, this is the best I can do. Realistically speaking, there is no hope for me, is there? There's no hope for the kid who's stuck at home with the AOL-Head family, and can't break through because he's not the financial decision maker.

My assets are: a brain, drive, and a lust to know what I can and can't do with this computer. Is there anyway I can learn to hack with what I have?

Ash

Hello Ash. First, let's define the word "hacker" so we're on the same page. According to www.wikipedia.org, an excerpt of what we typically believe to be a hacker is:

"hacker is extended to mean a person who makes things work beyond perceived limits through their own technical skill, such as a hardware hacker"

In other words, a hacker is a skilled user of technology, capable of modifying said technology to conform to their own needs. Given this definition, breaking into systems, vandalizing computers and wreaking havoc in any way isn't what we're about. If you can swallow this ideal, you're off to a good start.

Most of the hackers over here started with much less than you have at your disposal right now. We had 8-bit computers, no hard drives (some of us didn't even have floppy drives!), no internet, our modems ran at 300 baud (or even 110 baud for some of the extreme old schoolers).. So, you've got it good compared to where we started. With this in mind, here are my suggestions on how to learn to be a hacker.

1. *First and foremost, READ until you eyes feel like they're going to pop out of your head. … then read some more. Research every aspect of technology—computers, electronics, gadgets, etc. Don't limit your*

reading to the internet, although it's an excellent resource. In addition to this, you should pick up a few subject-related magazines (blacklisted, 2600, binary revolution,

2. *Learn to program multiple computer languages. I would recommend BASIC, C++, PASCAL and PERL for starters. Heck, why not even start with some simple HTML. I know it sounds like a hefty workload, but once you get the hang of one, the rest should fall in line rather quickly. It's important that you understand computer languages on some level before you understand how to manipulate them.*
3. *Ask a lot of very specific questions. Stay away from generic, "how can I be a hacker" questions, rather ask pointed questions about a specific topic. Ie: I need a piece of code for a programming project that will do THIS. You're more likely to get a sincere response if you appear that you really want to learn instead of having all the answers handed to you. You see, in the hacker community, it's important that each of us has the desire and capacity to learn and teach ourselves. It's part of the gameplan so to speak. Being self-taught is the hacker way. I believe black hat, white hat and gray hat would all agree on this point.*
4. *In addition to #3 above, if you do have a specific question, first look it up on Google before you pose your questions among the hacker community. Many times you will find that the answer to your question has already been asked—and answered—many times over and a simple search will reveal this to be true. Many "newbies" have been scom for failing to perform this rather easy task before asking their question. Be forewarned, hackers tend to be impatient when asked something that's already been answered. I believe it's just one of those bad traits certain groups exhibit. Naturally, you will from time to time, find more patient hackers who will hold your hand through the tough parts. Many hackers, sadly, do forget that they too started knowing little to nothing and had to put up with the same attitudes new hackers still have to deal with today. It comes from dealing with many wannabes, as you put it, who want it all but don't want to put any effort into learning.*
5. *Interact with other hackers. Find a local hacker meeting or attend DefCon, LayerOne, Toorcon, Interz0ne conventions. DefCon is by far the leader in hacker conventions and the best party in town. Not only will you walk away, learning something new, but you'll have an awesome time partying it up with other hackers. Additionally, you may want to try attending a local Linux or Unix user group meeting.*
6. *Visit hacker websites. I would personally recommend l-hacked.com. They're a hardware hacking website and I'm a big believer in hardware hacking—that's where all the fun is and the easy path for hackers to make something of themselves in the real world. Hardware hacking eventually leads to designing gadgets and doing honest hacker work. Hackaday. com is another cool hardware hacking website. Check 'em out when you have a chance.*
7. *Read hardware hacking books. I know I hard on reading, but it's really the best way to learn, aside from hands-on work. I would recommend these books for starters: Hardware Hacking: Have Fun While Voiding Your Warranty, Hardware Hacking Projects for Geeks, Home Hacking Projects for Geeks, Game Console Hacking, Wireless Hacking, etc.. All of these are interesting reads..*
8. *Build your own computer. People always balk at this comment. It's NOT impossible to build your own machine. If you're broke or cannot afford the parts, go to a local computer scrapyard or local computer repair center and ask them for some leftovers. I didn't say build a new top of the line Pentium 4, 5Ghz system. Try your hand at putting together an older 486 system (and, yes you CAN get the parts for free—I see the ads in the local recycler all the time, "please come and take this crap away!!")*
9. *Post in hacker forums.. Again, if you have questions, be SPECIFIC and pointed. No generalized questions. Hackers don't want to spoon feed you all the answers, they want to see that you're genuinely interested and trying to learn on your own. Binary Revolution has a really good forum. We have a forum, too.*

So, that's about it. Give all these steps a try and see where you go. There's no magic pill that will turn you into a hacker overnight. It takes time, patience and a lot of aggravation. Just stick with it and, eventually, you'll get onboard. Good luck.

In regards to the info Lint requested in Volume 6 Issue 4: I used to work for the company that manufactured the BART cards, along with cards and tickets from transportation systems all over the world. Unless they have changed in the last five years or so the BART cards are Low Coercivity, 300 Oersted. The 0.25 inch magnetic stripe is applied directly to the card extruded from a slurry of magnetic "ink" that we manufactured ourselves. Our job in production was to apply the stripe in the correct position and to the specified electrical properties which we tested by writing a signal to samples and reading back the return on a digital scope. There were many other parameters to deal with making for a hair pulling experience. These contract jobs are offered by a sealed bidding process, so what's made by one company today may be made by another next time around. The manufacturers of the equipment the tickets are used in design and quote the specifications of the product and it is up to the supplier to deliver cards that meet or exceed the specs. Hope this helps.

Dark Purpose

Hey Dark Purpose. Thanks for the input.

Ok, so I was sitting in Computer class... I know what your thinking he hacked into his schools computer, But really I was just bypassing my school Internet restrictions on the Internet using Firefox.

1. First thing you want to do is find out the kind of stuff your school is blocking on the net.

2. Go out and buy a USB Key (128MB+)

3. Download and install Firefox to your USB Key

4. Download and install plug-ins (Flash player)

5. Rename Firefox to Internet Explorer on your USB

6. Test and run Firefox to see if it works. Don't save any settings.

7. Take your USB to school/work put in USB slot on a computer at your school/work and run Firefox now your going to want to transfer all your stuff from Internet explorer when it ask, then it asks if you want to make Firefox your default browser, click NO.

8. See if any sites load and work (They should work and you should be able to play games and download stuff)

Now that you did those steps Or I hope you did, or if you don't understand some of the steps I'll tell you what is going on in each step.

In step 1 you want to gather all the info you can about your school computers and how the network is setup and what it blocks and what runs. Try downloading things and running things. In step 2 you need the USB so you can install Firefox (In step 3) most USB keys at 128MB are around $19.99 . In step 3 you will download and install Firefox to the USB so you can run it on the computer. Reason it's on a USB and your installing it at your house is because most schools or

work areas block download and installing things. In Step 4 you want to get all your plug-ins for Firefox so you can play your games or download your emulators :). In Step 5 You want to rename Firefox because most schools keep a log of every program you open, Most only show the name of the program your running and not an Icon and details so if you rename it Firefox they think your on Internet Explorer. In Step 6 You want to test and run Firefox at your house (run it from your USB only) so you can see if it's all working and running fine. In step 7 you finally get to take it to school or work and put it in the USB slot and run Firefox (now AKA Internet Explorer) and when you run Firefox it will ask if you want to transfer all your info from Internet explorer to Firefox, you want to click YES, Because this transfers the proxy info for Firefox to connect to the network and run. If you have to manually set the connection settings go to Tools> Options> Connection Settings and enter the info in. It also may ask if you want to make Firefox your Default browser, Click NO. In Step 8 you get to use Firefox for all your internet needs music, games, forums,.

You can try to install Firefox to your computer at school but try to hide it and also rename it. If not just use the USB options or put it on a CD and run it that way. But easy way to hide it I think is on a USB key.

The main reason I wrote this tutorial is because my school I had to use this because they turned off ActiveX and that stopped me from being able to play games (needed flash/ ActiveX), use online proxy sites such as www.cbrowse.com and www.whopy.com because the fields for entering the address were in JavaScript (needed ActiveX) and I had to use those to check out www.2600.com site for updates since it was a blocked site titled "hacking" :(. So I hope this helps other people with the same problems. Once I used firefox I could get on www.addictinggames.com and play games and visit proxy sites so I could bypass the school filter and visit my most Favorite sites!

Mixfever

Interesting work-around. Keep in mind that the schools install those internet restrictions for a reason and bypassing these restrictions may be asking for trouble—it depends on the school and how aggressive their rules are. We applaud the effort, but don't condone applying these work-arounds on the property of others. It's just a recipe for disaster.

Hi guys, great try. The Summer edition is almost worthless to me as I can't read the small type and I got tired of trying to use a magnifying glass. I even copied the pages using "enlarge" to try and read it. If you are going to have a larger print version out for Winter, I'll subscribe.

Dave

Hello Dave. This is a growing complaint that we receive about 2 or 3 times a year. Over the years, I have dismissed this complaint since it's only so few. However, I've recently taken this complaint to heart, not because of my own inability to read the magazine (in fact, I can read the text perfectly, but I have 20/20 without the use of any corrective apparatus) but rather the mounting complaints over the last couple of years coupled with our aging readers. Anyhow, me being a hacker and wanting to get to the bottom of the problem at hand, I went out and asked people what specifically generated problems with people reading the magazine. Upon further investigation, I was able to ascertain what the problem really was. Apparently, some of our readers have trouble reading Times New Roman at 6 point, but the Arial at 6-point is perfectly legible. So, because of this specific information, I have upped the Times New Roman a notch to 7 point from here on out. Hopefully, this will alleviate the problem. Only time will tell. I will watch for additional complaints. So, there ya have it Dave. And it didn't even have to wait until the Winter issue (this is the FALL issue). How's that for quick response time? Hope the jump in font size helps out.

I am investigating a scam operation and need to find someone who can:

1. Get an unlisted AT&T cell phone number
2. Get a SBC Global DSL e-mail address password
3. Construct an attachment that will install a file on an OS10.2 Mac when the file is received and opened as e-mail

Please contact me and I will verify who I am and the reason for this.

Bill

Bill, every time I read a question like this, I can't help but feel like someone's trying to pull the wool over my eyes, so to speak. Personally, I don't care what your reasons are for wanting to know how to do these things, the fact remains that doing these things are illegal, with the exception of item # 1 above. You can go to any number of sources, whom I refuse to disclose to you and find this information LEGALLY. Item #2 - this is asking for trouble. Computer trespassing comes to mind. An icky thing to do....and get caught doing. Item # 3. This one pisses me off. I hate SPAM, I hate virii (viruses), I hate worms, and I hate trojan horses. This is the kind of stuff that gets people in a HEAP of trouble and I don't feel sorry for them. Not one bit.

I can appreciate wanting to shut down a scam operation, but I absolutely do not condone breaking the law to accomplish the task. It's bad for your own personal freedom and it's bad for the hacker name. Every time someone does this crap, hackers get blamed for it. I for one won't help the media in their efforts to discredit the hacker community.

I have been a fan for awhile and was looking to subscribe but when I noticed that your magazine has seemingly disappeared from the local book shops since the Winter 2004 edition. I also noticed that the website hasn't made mention of a newer edition since then either and it appears that you guys have abandoned the website as well. I have only seen updates and posts from readers and nothing from the staff since last year.

WTF?!! Are you guys going to publish this magazine or are you going to go the way of Phrack and so many other great hacker mags and just disappear? Don't let 2600 be the only remaining 'real' hacker mag out there. Let the readers know what we can do to help you out (other than subscribe -- seeing we may not see another magazine). I'll keep buying them off the shelf and telling people about it as long as you'll keep putting them on the shelf to begin with.

I hope you're still out there somewhere to get this message.

Shard66

Hey Shard66. You and I have had some words back and forth in the forums and I know the record has been set straight as far as you're concerned. I thought I would go ahead and include this comment in the latest edition, just to clear the air for everyone to read. In a nutshell, two problems occurred over the time-span that the Winter 2004/2005 and Spring 2005 issues were to be released. The first problem was a lack of redundancy with our printer services which ultimately caused the Winter 2004/2005 issue to go unpublished. I know it's a shame, but we sucked it up and took the punches as they came in and still got the next issue out on time. Which brings us to the Spring 2005 issue. We printed up 150,000 copies and was ready to release the issue as planned. However, one of our long-time distributors (Desert Moon periodicals) went out of business, taking with them crucial distribution into a couple of high profile chains. We scattered to try and fix the problem, but in the end, our Spring issue missed some important distribution into two chain stores which didn't make us look any better. Anyhow, by the Summer issue, we had shifted our distribution to another company and the problem was resolved. Shard66, I

know you already verified distribution into your area which is good news. Sadly, the length of time is takes from the day we ship to the day the issue appears on the shelves is completely outside of our control. Each issue for the next two years, we're planning to release a week earlier than the full three months between issues. By the time 8 issues pass, we'll be back on track, getting our issues out well BEFORE each new season starts. It's a simple, yet effective plan.

So, to sum up, we're still in biz and everything is fine. Our Spring 2005 and Summer 2005 issues both saw heavy distribution, even with the distribution company problem for the Spring 2005 issue. We were steady at 150,000 copies for the Spring and Summer issues. With the issue you are now holding in your hands, we're at an astounding 200,000 copies! I think it's safe to say that we're in fact the #1 distributed HACKER magazine on the planet. Not an easy thing to accomplish, either. Yay for us.

As for our website, please note the massive changes we've made recently. Go check it out if you haven't already done so. As far as helping out, as always, we can use articles, artwork and photographs. That's pretty standard. Some people have already stepped up to the plate and put forth their support. Thanks guys!

Hello, I got a free issue of BL411 at DefCon and enjoyed reading it on the plane ride home (although it is about 6 point font--maybe we could bring that up to 10 point, huh?)...I went ahead and signed up for a subscription. I can't wait to see the DVD some day.

BTW, my wife and I especially enjoyed the heartwarming article by the chick who married the hacker. Pretty funny--and true.

Hello. Is there a number or something of that nature that would help identify your magazine to the person that does the purchasing for the stores ?

Brian

Hello Brian, yes, tell them the ISSN of the magazine you're looking for is 1082-2216. Further, you can use the BIPAD which is 40535 or the full barcode which is 5064440535. What store are you dealing with? We may be able to help from this end.

What I would like to see would be a very thorough tutorial about the DC Capture the Flag competition. Exactly how does it work, what t00lz/skillz do you need, how do the referees score & monitor everything, who are some of the top playerz, how do you get involved with a group that does this, do the playerz practice together all the time or just get together at DC, etc. It looks like a lot of fun, but everyone's working so hard, you hate to bother them trying to get some answers.

Thanks and keep up the good work.

JeremyCEC

Hello JeremyCEC. Thank you for your comments. We try to provide an interesting media for our readers so I'm always happy to hear when someone enjoys what we offer. I'll forward your comments to Zero Hack about her article.

Anyhow, about the font size. We get about 2-3 complaints per year on this topic. We've fiddled with the font size from time to time but the very "small" size tends to lend itself to getting more information crammed into each issue. You'll be happy to know that we have upped the font size ever so slightly with the Times New Roman (by one point) so we'll see if that helps at all.

The DVD. We're so close to having this done. You'll be able to get this online as well as from any number of major retailers. We're very excited about this project over here.

DC Capture the flag. I'll see if I can get someone over here to write something on this topic.

Thank you again for your time and comments. If you have any other comments, feel free to contact me anytime.

Hey, I remembered an ad in one of your 2000 or 2001 issues for an electronics surplus store in California. I cant remember the name...maybe you can help me out? I can remember the place having a website. Heh, that probably doesn't help much. Lemme know if you can remember

Fermicirrus

Hey, first off, we weren't publishing in 2000-2001, so your dates must be off. We've talked about many surplus stores in CA as well as placed ads for them. Since we're west coast, most of the places we deal with are local to us, so it's difficult to narrow down what you're looking for, Can you be more specific?

I have three questions that maybe you or one of your readers could explain.

Question 1: How do I modify my Nextel (Motorola) phone? Does the model of phone change how one would go about modifying the phone or trying to access a forgotten password?

Question 2: How would someone who wanted to gain access to the continuously broadcasted satellite television without having to "pay" for it? also how would one go about amplifying the signal to distribute the signal to other rooms so that their is no longer a need for the in room equipment.

For that matter how could someone get around a cable box for the home that is required for "HBO" and other "pay" channels

Question 3: My third question is with a laptop with WI-FI capabilities. How would someone go about building a directional antenna for better reception. More importantly is there a way to "boost" the output of the send/receive signal to improvement of the WI-FI signal?

BL411

For question 1, go to www.motomodders.com—they have all the latest Motorola phone hacks and mods.

Question 2. Sorry but we're not in the business of stealing satellite or cable programming. That's outside of our arena. Although, amplifying the signal to all of your rooms throughout the house, you could use a distribution amp from the output of your receiver and hardwire all the rooms to the amp.

Question 3. Directional wi-fi antennas are available all over the net. If you want to BUILD your own, check out the review article on our website. www.blacklisted411.net which describes a site dedicated to building your own directional antenna. Can you boost the output? Sure you can. Visit www.omni-wifi.com or www.wifiantenna.com. Both of these sites have interesting gear available. For the boosters, be prepared to spend some money. If you want to go on the cheap for a signal booster, a company by the name of Hawking makes the model HSB2 hi-gain WiFi signal booster. It runs about $50-ish. I have not reviewed one of these yet, but I've heard mixed reports about it's usefulness. The manufacturer claims a maximum distance boost of up to 600%. That's worth a gander.

Well mates, the only way to find your magazine is to come in US, is bloody difficult to find here in Italy! I'm lucky, I used to travel often for working reasons, so... voilà, just caught the Summer issue. You guys do a great job, tks indeed!

M@rkus

You're absolutely right. We don't have any distribution into Italy. At least, not that I am aware of. We'd like to change that. If you have a listing of specialty stores that carry interesting publications from the U.S., forward the information and I'll see if we can't get our magazine available in your location.

A friend and I will be starting a monthly meeting in my area (40 miles east of Pittsburgh, PA). We would like to associate the meeting with Blacklisted 411, especially your group's ethos of 'information should be free' and 'knowledge should always be shared, even with noobies'.

The purpose of these meetings will be to gather in one place people in the area with similar interests and give them an opportunity to talk, share ideas, discuss projects, and maybe even teach / learn something. We will be putting up flyers and creating a website over the course of the next month hopefully with the first meeting taking place in about 4 weeks.

I think I remember (haven't read my first issue of Blacklisted since Defcon some weeks ago) mention in your mag about emailing you and you could provide guidelines of sorts for holding such meetings. I was also hoping that it might be possible to purchase additional copies of your magazine, perhaps 50 copies (at a discount?), to distribute and help stir-up interest.

Also if you have any flyers (PDF, JPG, whatever) that could be modified and used it'd be great!

Jpbarto

Hello and welcome aboard. I'm glad to see more and more people interesting in starting up their own meetings. We'd be happy to help in any way we can. We don't have any pre-made flyers since we don't host meetings ourselves, but I'm sure you're more than capable of producing your own flyers. Anyhow, if you need copies of our magazine, contact me via email. Last but not least, send over the specifics on your meeting—where it's to be held, what day of the month, etc. I'd be glad to add it to our meet listing in the back of the magazine. Good luck!!

Hi, I'm Rudy and i just started reading your magazine and I love it. I'm also just starting to learn how to hack. I think it's just amazing what hackers do for people. The thing is that I don't exactly know how to do it and i was wondering if you could e-mail me with some advise on how to manipulate codes and to blow security. The whole reason I started to hack is because my parents keep on putting passwords on my computer and I cant get through the code. So help a guy out and a new hacker to the hacker society :).

Rudy

Hello Rudy and welcome aboard. First off, we don't email responses to questions like these—we print them in the magazine. Second of all, we don't show people how to hack, that's something you will have to learn on your own. We can help you along the way, however. Hacking isn't about blowing security, well not exactly. It's about exploring the possibilities that exist in and around technology. I just answered someone else about becoming a hacker. The same applies to you. Good luck.

Dear 411 and Roman H, Awesome mag, you guys have outdone yourselves once again. I grew up in the Atari and Commodore 64 age. I fondly remember sitting in front of the C-64 with a copy of Compute entering lines of basic.

Roman H, MAME is awesome, you can get all the information you need about it from a few websites.

Do a Google search for the group alt.games.mame where you'll get all the updated news and frequently asked questions.

http://groups-beta.google.com/group/alt.games.mame - here you can get additional files to make it run better.

http://www.classicgaming.com/mame32qa/ - I recommend mame32, it's easy to install and one single download. finding the roms is different, you'll get a few of those here:

http://www.tombstones.org.uk/~ankman/

When I'm not on the computer hacking or playing MAME then I'm on my brand new Atari Flashback 2 which is based on the 2600 system with 40 built in games. I have an awesome time playing it and get the manuals for the games from www.atariage.com. Yeah this sounds like a commercial or advertisement.

I am looking for an emulator for the C-64, I'm looking for an air traffic controller game and my wife continually asks me to find "TOOTH INVADERS" for her. Any help here?

Thanks again for an awesome mag, keep up the great work.

Superman

Hey Superman. Good to hear from you. Thanks for the update to Roman's question. I loved the Commodore 64. In fact, when I first made the Blacklisted 411 hacker monthly in 1983, it was on a Commodore 64 and released on C=64 diskettes. Boy, the memories. Anyhow, Air Traffic Controller by Hewson as well as Tooth Invaders by Commodore are both available all over the net as a ROM image (for use with emulators). If you want the actual software on floppy disk, or in the case of Tooth Invaders, on cartridge, you might want to try Ebay. As much as I despise Ebay, I have to admit that they make it pretty easy for people to find obscure items that otherwise would be nearly impossible to locate....naturally, for a premium, with some exceptions of course.

Hi, I picked up a copy of your mag about a month ago at Cinefile Video (Vol. 6, Issue 4, "Hacking with a proxy server"). It caught my eye because one of my roommates is into animatronics, and I'm experimenting with Unix by putting NetBSD on my old Powermac 8500. I saw in the Black Market section that you're looking for an artist. I happen to work as a graphic designer, and I do illustration as well. You can find a PDF of my portfolio at <deleted> (you'll have to excuse the website, though. Web is not my specialty.)

It's not really finished yet, but perhaps you'd find it interesting. I don't always have a lot of time in between working and looking for work, but I thought I'd offer my services in case you ever would want to take advantage of them. Anyway, keep up the good work!

Erik

Hey Erik, thanks for the heads up. We're always interested in new graphics work. When you have a chance, can you send your sample work to us? Thanks for your support.

Hello Blacklisted crew. I am very impressed with your magazine. I like your attitude and the wealth of information you present to the readers. I specifically enjoyed the Serious Salvage series by TechnoHeap. I was wondering if you were planning on doing any updates to his salvage articles anytime soon? I buy up each issue, hoping you're going to include

more information on this subject. I'd like to thank you for the information because I was able to actually generate an income from his suggestions. That alone make you guys worth the read! I've been watching all of these salvage places since I read your first issue that included the Serious Salvage series. I'd like to update you that Ball Electronics and ACP have both gone out of business. Ok, well thanks for the awesome magazine. Keep up the great work guys!

Salvage Hound

Hey Salvage Hound. TechnoHeap has been working away at a new article for awhile now, complete with photographs and additional information on where to find the good stuff. You are correct. Not only has Ball Electronics gone under after dwindling patronage over the years, but the ACP retail store front has in fact gone toe-up. However, you'll be happy to know that ACP Components (across the street in a completely unmarked warehouse) is still in business. Yay. Also on the MIA list is: Marvac in Clairmont, Marvac in Pasadena and a couple of other smaller retailers. The surplus market, regardless of these closings, is alive and well. You just have to know where to look. TechnoHeap will reveal all in an upcoming issue. Stay tuned. I've forwarded your concerns to him.

Dear Blacklisted. I recently visited this website called "the flash mind reader" at http://trunks.secondfoundation.org/files/psychic.swf and it has completely baffled me as to how it works. Can you take a look and explain it to me? I know it's not really reading my mind, but it sure is a trip to see it correctly show me my symbol each time. Thanks guys, I love what you're doing over there!!

Charlie K.

Hey Charlie. This is a simple math trick. You're supposed to use digits 00 through 99. Given this and the equation they offer up, there are only 10 possible answers. Two digit numbers 00 through 09 will produce answer of 0, numbers 10 through 19 will produce answer of 9, numbers 20 through 29 will produce answer of 18, numbers 30 through 39 will produce answer of 27 and so on...40 to 49 is 36, 50 to 59 is 45, 60 to 69 is 54, 70 to 79 is 63, 80 to 89 is 72 and 90 to 99 is 81. As you can see, only 10 possible answers. The site knows that every time you do an equation (correctly), one of your answers must be from the above list. If you look at the site, each of the answers above (0, 9, 18, 27, 36, 45, 54, 63, 72, 81) has the exact same symbol associated with it. You click the crystal ball and that very symbol will show itself. Pretty neat, huh?

I have a question that maybe one of your readers or you could answer. The question is I have a friend who has a Phone from Nextel and the phone has GPS capabilities but the company wants a monthly charge to access it. Is their a way around that? Another question I have is that the same person wants to change their phone number on the phone but she bought if from someone else and the other person has forgotten the password how can she find out the password?

Reader

Hello. As far as bypassing a paid service, I can't help you with that at all. If you want to get into the phone, I would need to know the model number. Without that information, I'm at a loss and cannot advise you. However, you may want to try out www.motomodders.com - they have a tremendous amount of information on Motorola phones. I believe you might be able to find someone who can help you out.

Hey guys. I've been reading your magazine since volume 6, issue 4. All I can say is WOW!! I really am impressed with the operation you've got going on and your willingness to help just about anyone at any level of experience. I have a question for you. It's not really hacking related, but more on classic tech. You seem to have a firm grasp on where to find things, so I thought it couldn't hurt to ask you. I've been working on some old Atari Star Wars boards (arcade game) and I've run into a situation where I need some spare POKEY chips (you know, the C012294B sound chip). I found a stash of boards at an operators location but the boards were stripped clean of the socketed chips. I was able to locate everything (including the EPROMs and speech chip) but I've been unable to locate that damed pokey chip part number anywhere. I know this is a lame question, but I really need this part so I can revive at least one of these machines. I heard that you can find them in old cartridges of some type. Is this true? Which ones? Ok, well thanks for your help. If there is anything I can do to help out your cause, let me know.

Jasper

Hey Jasper. Listen, this is an easy question to answer. If you want the pokey, best place is to visit Best Electronics at www.best-electronics-ca.com). Last time I checked, they were going for $5 each. Not too bad, really. As for finding them in cartridges, yes this is true. You can find them in two Atari 7800 cartridges: Ballblazer and Commando. Note, they are NOT socketed and you will be required to desolder them from the circuit board. In my opinion, I would just pay the $5 and avoid the hassle of having to desolder (and possibly damage) a 40 pin chip. Good luck. Those Star Wars boardsets take 4 Pokeys each. That can add up real fast!

In the online article "Finding and Using Anonymous Proxies" by Hevnsnt, I had some trouble using the Charon application that he described. I am having trouble with finding a valid "Proxy Judge" in the "Connect Options" box. It always sez "Bad Proxy Judge Detected" when I enter a proxy there. I beleive that this is why I cannot find anonymous proxies using Charon. Can you help me with this?

Brainwaste

Greetings Zach. I know you guys are deep into component level design and repair. I've been trying my hand at component level repair and have one huge hurdle I've yet to discover an easy way to get around. Desoldering. Yes, desoldering chips from circuit boards without destroying the board. I've tried solder suckers. I've tried desoldering wick. I've tried heat guns. I always find a new way to destroy the circuit board in the process of trying to remove chips. HELP!

Destiny X

Hello Destiny. I was just having this very conversation with a staff member a few weeks ago. Here's what I recommended to him at the time. Get yourself a professional desoldering station. I personally recommend the Hakko line-up. Www.hakko.com I would go for the model 701 (http://www.hakko.com/english/products/hakko_701.html)or an older 700 if you can find one. They're really great little machines. Note, stay AWAY from the model 808. Using the 700/701 is pretty simple as long as you know how to go about it. First, flow some new solder onto the pins of the chip you want to remove. Then, use the desoldering part of the hakko unit. Place the tip on the pad, heat it up until the solder melts, move it around a little to make sure the solder has melted in the hole, then squeeze the trigger. SUCK... solder all gone. Do that for every pin and the chip should come up with little trouble and no damage to the board. I've done it thousands of times without ever losing a board (or a chip for that matter). I did a quick look and found a new model 700 on ebay for $100 buy it now. Not a bad deal at all considering this unit runs about $900 new. Oh, be sure to change out the filters OFTEN. They get clogged up, usually after you shut the machine down and it cools off. I usually change them out just before I start the unit up each time. Good luck.

I am trying to access some data on a disk. I'm having a hell of a time with this. Is there any way to can help me?

Greevil

Well, we'd like to help you, but we have no idea what you want help with, exactly. What do you want to access, precisely? Do you need to get some data off of a dead hard drive? Do you want to remove some data off of a floppy which is from a different platform than your own? Do you want to "rip" some code from a game on disk? What? We're waiting to get a more detailed idea of what you want help with. Data on a disk....I can assume you mean a 3.5" disk on the PC platform. But, then again, I could be wrong. I really need more information on the subject before I can advise you.

I am having one hell of a time over here! SCE has turned off my power and I'm pissed off. They want this HUGE deposit before they will turn the power back on. What are my options here? Can I just file a dispute and get my power back on? I'm sure you can give me some insight. I've been without power for nearly a week and a half now. HELP!

Powerless

We hope you have your power back on by the time you read this! Answering your question, unfortunately there are not many options available to you. As you know, SCE and other utility companies are nothing short of monopolies. So, let's see here. I'm assuming you failed to pay which is the initial cause for your un-plugged status Now they want a deposit plus any monies owed. Typical.

Ok, here's the deal.. If you dispute them, call up the Public Utilities Commission and complain. They will require you to give them the money in question and then they will decide who is right and who is wrong. Unfortunately, we must inform you that the PUC is in the back pockets of ALL the utility companies. Yeah, PUC, we know they own you! Don't try to lie your way out of it! So, in essence, you just waste your time and SCE gets the money anyway. I've never once witnessed any individual or company win against a utility when the PUC is involved. Never!

Anyway, if you don't want to bother with them, you can just pay SCE.. It's not lost money. They will hold the deposit for a length of one year and then, if there are NO late payments within that year, they will credit your account with the deposit amount, plus any interest made within that year (the interest is supposed to be whatever the prime rate is at the time - which amounts to nothing, really) According to their rules, if you ARE late any time within that year, they reserve the right to hold on to that deposit for up to 5 years. That's what they say, but in reality, they just start the 12 month clock over again.

If you disconnect service at any time and you are paid up at the time, they will refund your deposit. The deposit isn't such a bad thing unless it's outrageous and you just cannot afford it. If that is the case, you might want to try calling Home Energy Assistance. They may be able to help you. Their number is (800)433-4327. Who knows, you might be eligible.

Your last option is theft, which we do not encourage, but it is a thought which crosses many minds. Theft of power has a hefty penalty and it's dangerous. However, it's very easy to do - and - get away with, believe it or not. You can slow meters down, tap power off of a neighbor, etc..

My suggestion is to pucker up and pay SCE. I know it's not what you wanted to hear, but we're not about stealing services. SCE workers can be really nice if you show interest in paying them. In fact, if you ask nicely, they may reduce the "deposit" amount or push the deposit back to a further date, let you make installments on it, etc. Under NO circumstances will they ignore the deposit. They're going to make you pay it, no matter what excuse you may have. It's a simple but sad truth.

In the movie, "War Games," Matthew Broderick is able to trick a telephone into giving him a free call with a soda can pull tab & trick an electronic lock into opening with a tape recorder. Are these plausible? Can you explain them? Devoted reader in Cambrige, MA. P.S. Please use larger text in future issues. P.P.S. What's a COCOT?

Unknown

Ok, here we go.. By the way, we really do love this movie.. it's one of our favorites over here.. All of the details of the stuff they do within that movie may not be entirely correct, but when you overlook those minor(HUGE) details, it's a fun movie to watch. Anyhow, on to your questions. It is entirely possible to "fool" a payphone into giving you a free phone call - in essence, making the phone believe you inserted money when, in fact, you did not do so. The method Matthew used to achieve this is has never successfully been attempted by anyone over here, though we have heard over and over again by many that it did in fact work at some point in time, supposedly still working about the time the movie came out.

The next question: Matthew tricked an electronic lock into opening with a tape recorder. Now, again, this is entirely possible given the information we had at the time of watching the movie. You can clearly "hear" in the movie that the keypresses did, in fact, create a DTMF tone with each push. A recording of these tones would most likely be readily acceptable into the input of the electronic switch. However, it was a very crude, CRUDE example and there was no isolation used, etc.. Anyhow, I doubt very much that NORAD would be using such crappy security locks on their detention (looked more like a medical unit) cells. Every single electronic lock that we've worked with never EVER used DTMF tones to operate the switching action. However, we do know there exists switching devices that DO use DTMF tones (over the phone lines or over Amateur radio auto patches) to operate. Given the type of switch used in the movie (a DTMF operated switch) it was possible to trick it as done in the movie....however, unlikely that the real world uses such locks in locations such as the one in the movie.

Explanation: In the movie, the switch used DTMF (Dual Tone, Multi Frequency) tones (such as the tones made when you push keys on your telephone).... these tones, in turn, operate the switch....the switch is "listening" for those tones.. when it hears the proper sequence, it opens up. Now, simply recording these tones would suffice in fooling the switch. Record the tones and then play them back... it'll be nearly the same as keying in the tones by hand.... that's it. Try this... next time you make a call, figure out a way to RECORD the tones you're dialing. When done, play the tones into the mouthpiece at a later time.. If you recorded them with any clarity and play them back with little distortion and high enough audio level, the call should be placed as if you just dialed it by hand. Pretty neat! haha.. This is how people used to (and still do, actually) place redbox phone calls. They record the coin insertion tones and then play them back into the mouthpiece of a payphone somewhere. Although many phone companies have caught onto this and it no longer works as the mouthpiece is shut OFF until a coin is inserted, at which time you CAN use the recorded tones... Fun! Doesn't always work, as there's always someone doing something new to stop call fraud. Ok, as for larger text in the future? We'll work on it.. We have to cram a LOT of stuff on these pages, larger text would seriously cut into the content quantity.. We'll see about it, though.

A COCOT is a Customer Owned Coin Operated Telephone.... it's a payphone that you or I or anyone can purchase, pop onto a phone line and make money with it.. These phones can be found all over the states...and they are not operated by the phone companies... They are privately owned and operated... That's about it. Happy hacking!

I just wanted to compliment you for running a great magazine. I thought that your answers to the guy who was still using a Commodore 64 home computer were right on the nose and it was nice of you to refer to the machine as you did. I get sick of people talking down on the Commodore 64 all the time. As you know, it was (and still is) a great little machine and does a lot for such a small (and OLD) piece of work. I was wondering if you could print a little more on the Amiga line of computers because I recently purchased a used Amiga 2000 and I would like to know more about it, how I can use it, what software I should use with it, etc. Thanks for a great mag!

Hawkeye

Hey Hawkeye, we've been trying to include articles on the Amiga as often as possible. We still get a few requests for them from time to time and then we pump out a new article. Most of them have been done by Mobby G. as of late. He's our only Amiga writer we have around. Anyhow, we will, in future issues, be dealing more with the hardware hacks and such and how you can use it in a manner which follows with the basic idea behind the magazine (hacking) more or less. Thanks for your interest in the growth of the magazine, Hawkeye..

I have an old Commodore 64 that I still use and I was wondering if there is anything I can use with it to learn a little more about hacking, phreaking and such. I am new to all of this, so please try to keep it simple like you usually do. By the way, I really do like your magazine. You guys are doing a great job!

PolarSwirl

You're in luck. A lot of us started out on Commodore 64's so we know of many things you can do with it. The only thing I will talk about this time around will be a program called "Phone Man" (I believe that's what it was called - it's been a LONG time) Anyhow, this cool little program has all sorts of stuff that's cool to play with.. It has a redbox tone generator, a green box tone generator, silver box, blue box, etc. Plus, it's a terminal software as well. Believe it or not, recording those little red box tones and playing them back into a payphone is what got a LOT of kids started in the wonderful world of hacking. Phone Man is a very OLD program and I do not know what the last release version of it was, but it will always remain in my mind that I had a good time playing with that program. There are many other programs you can use and a lot of little hacks you can make to do just about anything you can dream up. Locate that program, play with it for awhile and then get back to us. Have fun and hope you CAN locate the program.

This is the first time I've seen your magazine. I saw it in my local Borders, right where a competitors magazine (no names) used to be. I am happy to have found your magazine - it's pretty cool and has much better topics. Question: I am interested in submitting some articles for reprint. Would you be interested? Please withhold my name/location as I am sure some people may be offended with my association with you and I don't feel like dealing with them thinking I've left them in the dust for your magazine. It's a bunch of b.s., apparently! Anyhow, be sure to answer me and I'll get you some cool articles.

(name withheld)

Cool. Yes, we're always interested in article submissions... Contact us through our website ASAP and let us take a loot at what you've got. We can withhold your name/location, etc... BUT, if you're a writer for who I think you are.... you shouldn't CARE what they think.. If you still want to submit anything, try to include some type of name or alias that people will know. Our readers like to know who's articles they're reading. The more known you are, the better off your articles will be received. At least, that's how I see it. I suppose I could be completely off-base. Well, thanks for your support.

Just wanted to drop you a note and say how much I liked your mag. I had never heard of it until i was in my local Borders looking for the latest <other mag> and there weren't any and they seem to have stopped carrying them. Instead in it's exact place I see your magazine. So I see it say the official hackers magazine and take all 3 copies that they had in the store for my friends. I am an ex-hacker from back in the day when they got more than stealing cable accomplished and went to taco bell. Now all the so-called hackers do is smoke crack and talk a lot. Anyways, I am also about to start a store dedicated to hackers and hacking types of materials. It's called legal to me and have been selling console copiers under the name for a couple of years now. We well be a cross between a spy-shop and a computer store doing upgrades, software sales, cd-rom burning, selling all kinds of underground publications, and most every kind of semi-legal hacking paraphernalia that I can get my hands on. So if you could, can you send me info on advertising as well. Until now I didn't know there were any other magazines to contribute to. Anyways, thanx for a great mag and lots of luck in the future.

DoD

Hey, glad you like the magazine and we're happy you found it. Ah, how many times we're heard the same story... I found it at Borders...next to, behind, in front of, etc... <insert anonymous magazine name here> hahaha So, did your friends enjoy the copies you picked up for them? Glad to see someone from the old school hacker crowd is still around. When you start up your store, let us know. I'd like to check it out myself sometime. Check out our website (we just redesigned it) for your media kit information. Everything is available online now. Anyhow, I'm glad you hooked up with us. Yes, there ARE other hackers magazines available. Thanks for the comments. Be sure to contact us soon. We have a lot to talk about. Laters and take it easy.

With the massive influx of WWW users and AOLers, many of you may have noticed the surge in new 'ELiTE' haxors. I've got nothing wrong with this. I welcome new users into the scene when I can, and I hope they do well. Traditionally, they tend to be nice at first, till I ask them one question. From that point on, I am somewhat considered the enemy.

They get offended. Now, I am no old school hacker, but I am an old school user. I have had friends excel in the ANSI art field. I have had friends get busted for phreaking, hacking, carding, you name it. I just merely watched it all. But in the height of my AC, I noticed something. We were living in a golden age. Boards ALL ran without PCRs, UL/DL ratios, no file points, etc.

This subculture used to be about the free trade of information. It used to be about helping one another. I don't know what happened to that. Somewhere between _WarGames_ and _Sneakers_ something went wrong. The people that make up this mystic world of ours have gotten greedy. They all seek power, instead of companionship. You must know what I am talking about... Users aren't as nice anymore. The perpetual newbie is treated like shit by the users who think they have been in the scene a long time.

There shouldn't be a place for braggarts in our world. We visit a place where skin color and other material things don't matter. But the influx of users are making it matter. Like I said, I am no power user, and don't ever aspire to be, but this world of ours, this 'scene' is dying. I plead to you all not to let that happen... Make it about information, not who can get the most '0 days' first. Thanks 411, and you rule.

MetalHead

Times change — and the people change with it. We remember the "good old days" as well. We're in agreement that the whole scene has degraded over the years. People have become careless, rude and greedy. Once upon a time, one could call their local system and grab all the info they wanted, ask all the questions they wanted and someone would help. A little time passed and the people in the "know" started hoarding all the information for themselves and held onto it very tightly. If you had a question to ask, you were considered a "lamer".. This such behavior has been getting worse through the years. Now, it's come to a point where there are people who KNOW and the people who do NOT know.. not many people in between.

We're right there in the middle, guys. Helping people along. Bringing them into the know. If you don't like it, that's too bad. We're here to bust the information lock-up wide open so everyone will know what's going on. We're going stay to the true hacker ways and SHARE our informatic:n.

Ok, that's enough of that for awhile.. Thanks for bringing some topics into light. We all know it, but nobody wants to admit it. Thanks for being honest. We could use a little more of that. Ironic, isn't it? Hackers. Honesty. Doesn't seem like those two words should be anywhere near each other these days, considering that the media has been dragging the hacker name through the mud for many years.

Hey Blacklisted. I've heard about this Real ID thing (national ID card?) and I was wondering what your take was on the subject. You seem to have an unnatural ability to see right through the BS and give us the real scoop on any given subject. So, can you give me a heads up on the situation before I this new concept becomes a reality.

Sam B.

Hello Sam. Real ID. It's a up and coming "plan" (recently passed under the Real ID Act) to replace our drivers license with a new ID card which is supposed to be conformed to a standard that each and every State in the union can read electronically, more or less. The idea is to have a federally approved ID card in place for people who want to: travel on an airplane, open a bank account, collect social security payments or utilize any number of other governmental services. ..and, of course, this would supposedly make it more difficult for terrorists to do their evil bidding.

Well, I have a problem with a national ID only on a personal privacy issue, but on the surface, the ID sounds OK at this point. Overall, I have no issue with the stated intent, in fact it would be a good thing for all of us, particularly is you travel. Here's where it gets a little too hairy for my liking.

The Department of Homeland Security has been given the sole power to setup the standards for these ID cards. So far, we're pretty sure that the following information will be included on the card in electronic format: name, birth date, gender, ID number, a digital photograph and your address. The problem begins when we start adding retinal scan, fingerprints AND make it RFID compatible. It's possible that, eventually, the Department of Homeland Security may require this ID to be used to do your shopping at the local grocery store, the flower shop or who knows what else. The problem is that nobody knows and the Department of Homeland Security has sweeping power to do whatever the hell they feel like doing, with little to no opposition from any entity. The scariest part of this is the addition of RFID to the cards. I for one will refuse to use one of these up until the very end. The folks at defcon this year proved that RFID could be read from a distance of what, 69 feet was it? Could you imagine how tragic this would be for people? Have you ever heard of identity theft? It would get worse with these new ID's armed with RFID, not better! That's a fact, people.

So, all we can do is wait and see what the final details of this so-called "real" ID will amount to. I for one will be watching very closely on this subject. It's a real issue and everyone should be worried.

I've been following your magazine for a few issues and have decided to write in once and for all. I was at one of the surplus stores that TechnoHeap recently sugessted and I found a phone that had ABCD buttons. I was wondering what the A, B, C and D touch tone keys are used for? I have never seen them on anything else nor have I seen any mention of their use anywhere. Why are they not found on phones?

Grady V.

*Hi there, Grady... Ok, here's an answer straight out of the Hacker FAQ concerning the ABCD touch tones: These are extensions to the standard touch-tones (0-9, *, #) which originated with the U.S. military's Autovon phone network. The original names of these keys were FO (Flash Override), F (Flash), I (Immediate), and P (Priority). The various priority levels established calls with varying degrees of immediacy, terminating other conversations on the network if necessary. FO was the greatest priority, normally reserved for the President or very high ranking officials. P had a lesser priority, but still took precedence over calls that were placed without any priority established. Today, the tones are commonly referred to as the A, B, C and D tones respectively; each of these tones use 1633 Hz as their high tone. These are found mainly used in special applications such as amateur radio repeaters for their signaling and control. Modems and touch tone circuits tend to include the A, B, C and D tones as well. These tones have not been used for general public service, and it would take years before these tones could be used in such things as customer information lines; such services would have to be compatible with the existing 12-button touch tone sets in any case.*

An interesting note: most modems will recreate these touch tones... instead of numbers, use ABCD... see if it works on your modem.. Kind of useful for your touch tone projects if you're worried about people using their phones to trigger your devices. Think about it. It's called security through obscurity.

I love the magazine. I'm not particularly adept but I'm still curious. I study various technologies from time to time but I tend to get impatient with textbooks and want to know how the electronic and mechanical things I live with actually work. Your magazine is great for that, although it's often over my head. This gives me some direction, though.

A local electronics store here in Gainesville has recently changed hands and the new owner has been cleaning it out. It used to look like a chiphead's basement. You could find everything from new ic's to old 60's computer tape drives there, mostly in pieces. I used to go there just to poke around. Anyway, the new owner doesn't want the old stuff around anymore and has been taking out the parts that he thinks he can sell and tossing the rest. He told me that he had dumped five tons of stuff in the previous three months. I have been making nightly forays into his dumpster since then and have now got the garage too full to park the car in it.

Generally I strip stuff off of circuit boards and put things together on a solderless bread board. I often can't completely identify the components but when I can I tinker with them. It's a cheap supply of parts and I don't cry when I cook something. My question primarily is, how do I identify what the components are? The ones with numbers I can sometimes find data on in a replacement catalog or the ARRL handbook, but not very often. Sometimes the shape of a part gives it away. Often, though, I have no idea of what some part is.

A poke around in the construction roll off where a supermarket is under renovation scored me four of the led matrix type of electronic signs, and I would love to get them working. They bear the name Litek and three of the four are model ISA4008. The other one is model SAT4008. They're four feet, four inches long and have led matrices on both sides. They have four wire power cords, two wires each for ground and two for +9 volts. They each also have a four wire phone cord jack. The circuit boards inside bear the name Litek Microsystems, inc.

My guess is that you work out your design on a computer and upload it to the sign, probably through some kind of proprietary bus slot card. It would be cool if I could program them through a modem though. Anyway, they have little batteries on the boards so I think they must have enough memory to hold the message and that you could use the same computer to program a number of them. I would be appreciative of any help you could give me.

Keep the cool magazine coming.

tofm

Awesome! You're interested in electronics. You sound like the rest of us over here. I really hate to hear about people dumping so much junk like that. I would suggest taking as much of it as you can. if you're a real hardware hacker type, you can find a use for just about every little part you can find.

Stripping parts off of boards is a great way to save money and allow one to become "fearless" when they prototype stuff because, like you said, who cares if you fry something, right? Back in the 80's, I used to do the same thing... I'd have piles and piles of circuit boards set aside just to strip for parts. There's one big drawback (besides it being so time consuming - which doesn't really seem to matter for the real hacker type ... or really bored type) anyhow, the draw back is that you're not really too sure if the part you stripped off of a circuit board is good or not. It really sucks when you work so hard to get a circuit designed and then prototyped... and then you get stuck into a debug mode for the next 6 hours only to find out an electrolytic capacitor and two transistors were bad the whole time. Damnit! Now, I won't keep used parts for very long unless I can definitely determine if they're good or not.

Want to identify parts? This is going to sound kind of lame, but get your hands on electronic catalogs. Particularly older catalogs from the 80's—ACP put out a great catalog with tons of pictures and descriptions. So did Jameco. Their older catalogs are the best! Now, don't gasp everyone. Get your hands on a Radio Shack catalog for starters. It has pictures and descriptions of parts. It's a good start. Next, get some catalogs from places like:

JDR Microdevices
1850 South 10th Street
San Jose, CA 95112
(800)538-5005

Mouser Electronics
11433 Woodside Avenue
Santee, CA 92071
(800)992-9943

MECI
340 E. First Street
Dayton, OH 45402
(800)344-4465
http://www.meci.com

Marlin P. Jones & Assoc. Inc.
P.O. Box 12685
Lake Park, FL 33403-0685
(800)652-6733

All Electronics
905 S. vermont Avenue
Los Angeles, CA 90006
(213)380-8000
(800)826-5432
http://www.allcorp.com

Digikey
701 Brooks Ave. South
Thief River Falls, MN 56701-0677
(800)344-4539
http://www.digikey.com

Contact these people and get their catalogs. It will help you out quite a bit. We have no info on your electronic signs.. Perhaps one of our readers will be able to send information you can use.

Cool zine you guys have. Quickly, I need a rundown of the DTMF tones over here in the UK so I can mess around.. Can you also include the redbox tones, if they exist? Thanks Bunches

Zer0 Kay

We don't get many requests for this info, but we have it on hand. So, no problemo, dude! Here's the DTMF tones. You should be able to figure out the chart below:

	1209Hz	1336Hz	1477Hz	1633Hz
697Hz	1	2	3	A
770Hz	4	5	6	B
852Hz	7	8	9	C
941Hz	*	0	#	D

Now for the redbox tones. The 1000Hz tone listed below is NOT a DTMF, it's a single tone. (Strange, huh?) Anyhow, supposedly, for this to work, you need an operator to connect your call. We're not sure of the effectiveness of this, but here's the info to chomp on. If anyone out there has any specific information regarding this, please forward it to us. Anyhow, here's your redbox tone:

10p Length 200 milliseconds. Freq: 1000Hz.
20p Two times the Above.
50p Length 350 milliseconds. Freq: 1000Hz.
1ukp Two times the Above.

The Art of Casual WiFi Hacking

BY JEREMY MARTIN

It is a cloudy Friday night and I am in the listening to another episode of 2600's "Off the hook" radio when the interruption of the phone catches my attention. I had been expecting the call from my colleague, because I needed help with some new proof-of-concept ideas for a penetration test I have the following week. During the conversation, we eagerly decided to head out for the night to Wardrive in the area. Wardriving is always a good excuse to test new programs and ideas. We position both laptops for optimal WiFi signal, easy access to the GPS devices, and secure them for the least amount of movement while driving. Right before we leave, we make sure the power converter is turned on, and the systems are plugged in. To cover all our bases, one laptop runs Windows XP Pro, NetStumbler, and Cain&Able while the second system has Suse 9.2 Linux with Kismet, Airsnort, Aircrack, and Void11. Using two devices with such different environments improves success while surveying WiFi in an area or "footprinting" them.

Wardriving
Also referred to as *"Geek's catch and release fishing"*, is the act of driving around and scanning for open WiFi hotspots. This is considered a sport in many circles and is growing in popularity across the globe.

Warwalking
Is similar to wardriving, but on foot. There are many PDA devices that will allow you to install wireless and network auditing tools.

Here is where the fun begins. After driving for a few miles, we enter a well lit street in the business section of town, and hear the ping of live access points every few seconds. Even though we have been doing this for years, we are both amazed at the percentage of companies that employ WiFi that do not implement any sort of encryption. This allows us to park and let Kismet do what it does best... passively listen to network traffic running over the 802.11 signal. We are able to map several subnets and gather other interesting information being broadcast to the public. At the end of the night, we were able to gather over 127 WiFi hotspots after only driving seventeen miles round trip. With this type of information gathered, playtime for hackers begins.

Wardriving is done for many reasons. Some do it for a social activity with friends. Others Wardrive as a community service to increase awareness, as a business model to secure for profit, or even the cause the dreaded criminal acts of spreading viruses, hack, or commit fraud.

The Gear

Windows system:

- Acer Aspire 1520 laptop
- Riklen GPS
- FM Modulator
- Windows XP Pro
- NetStumbler
- Cain & Able
- MS Streets & Trips

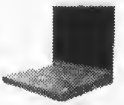
Linux system:

- Acer Travelmate
- Microsoft MN-520
- Suse Linux 9.2
- Kismet
- AirSnort
- Void11

Wardriving does not take a long list of special tools and equipment. Above is a list of equipment I use and have found to work, it is not a requirements list. Almost any WiFi enabled Windows machine can scan for hotspots right out of the box by installing either Cain or NetStumbler. Linux is another story. Since the Linux environment allows for more direct access to the hardware, there are more items to consider. These include Linux compatibility, correct drivers, and knowledge of iwconfig or similar configuration utility for using the card in promiscuous mode. Many "Live Linux" distributions take care of most the work for you if the WiFi card has compatible chipsets. The most common and well known WiFi chipset for Linux use is the PRISM 2. The Orinoco Gold card became very popular because of it's easy of use and ability to work with most Linux environments out of the box. You can use most Windows based cards in a Linux environment by using an NDIS driver, but they will not work for scanning purposes because of the inability to access the hardware directly.

The problem you may come across is that most Windows based scanning utilities use a method of scanning called "Active scanning" because of the limited access to the hardware. When scanning for WiFi using an active scanning method, your device sends out a request on every channel and logs all replies. The traffic produced can be immense and is also noisy. Anyone setup to listen for incoming connections will instantly know you are scanning because of this.

NetStumbler is an active Windows based scanner that produces the information you need for mapping WiFi hotspots including SSID, Encryption, and GPS coordinates. Since the program constantly screams out "ARE THERE ANY ACCESS POINTS OUT THERE", the responses are more abundant. One of the issues you may come across is that the traffic is so chatty that other devices scanning may get spammed by fake access points. NetStumbler is not self contained and it uses Windows drivers to access the WiFi card, causing the Wireless Zero Configuration to shut down when run. Wireless Zero Configuration in WinXP allows the operating system to find available WiFi networks. This is a problem for connecting to an access point while Wardriving. The easiest way to resolve this is to save the NetStumbler data, close the program, and refresh the available networks.



Cain & Able is one of the best FREE all-around auditing programs out there for the windows platform. It sports ARP poisoning, password crackers, a VoIP logger, and has a WiFi scanner built in. This application does not have the same downfall as NetStumbler because it uses a Third-Party driver called WinPcap (used for most low level network programs like the sniffer Ethereal). Cain & Able doesn't seem to detect the volume of Access points as NetStumbler does, so the choice is mainly a preference one

Kismet is popular because it uses "Passive scanning" methods and does not interfere with network traffic or WiFi signals. When using a passive scanner, data is logged only when an access point transmits. It is almost impossible to detect while giving you even more information then the previously mentioned counterparts. If enough traffic is generated or active traffic passes through, you can grab the IP address range of the access point without having to log in. Knowing the access point's IP address can come in handy if the network does not use DHCP. If you use a second computer running Cain to Arp poison the access point, Kismet can gather a lot more then just the SSID.

If you do not want to install a Linux distribution on your system, you can download a live Linux distribution with all of the required tools already installed on a CD. Live Linux distributions are used to allow even a Windows installed system to boot into a Linux environment that is not installed on the hard drive. Most Live Linux distributions do not mount the hard drive and leave little to no trace evidence that they were ever used in an attack. These distributions can also be used to gather information from a target system without compromising the evidence.

Last but not least, you need a means of transportation of some sort. I like to use a vehicle because I'm too lazy to carry around a "desktop replacement" laptop and have not invested money into a good PDA yet. It's much more efficient to sit, relax, and Wardrive. I drive a good old American gas guzzling SUV to seat all of the people comfortably. One of the most important items you can purchase besides the computer equipment would have to be the power converter. I use a three 700 watt AC converters because there are always 1-6 people needing power when ever I go out. I also have a spare battery because I tend to drain more power then most people.

Now that you have chosen your gear, you can start to Wardrive. One of the most common questions people ask when they are new to the scene is "what should I expect"? When you drive, most areas will usually have a concentration of noticeable signals in business districts and residential areas. I know it doesn't take a genius to deduct these obvious facts, but there are different reasons why the hotspots are available.

Small to medium sized businesses are more likely to have unsecured wireless access points then large companies, publicly traded businesses, financial institutions, or health organizations. The later are covered under many regulations in most countries and are required to encrypt wireless communications if they are allowed to use them at all. Many small to medium sized businesses either do not have the budget to hire competent IT staff or do not feel that the security is important and do not bother to lock down straying signals. Yet there is another reason this section may have open WiFi. They want it… Some people feel adding open internet access adds another level of service and quality of life to their environment. These companies welcome your patronage.

Residential WiFi is the most common signal you will pick up. Some open access points are open to develop adhoc Metropolitan Area Networks for file sharing, underground internet media, and to help make society. SeattleWireless.net is a prime example of a portion of the community working together to bring WiFi to a larger crowd. This Seattle based group even produced several online videos to help increase awareness. Not all residential service is open to sharing though. Many ISPs have service agreements that make sharing the Internet access against the rules, subjecting the owner to fines and/or cancellation of service. If the resident does not give you the proverbial "ok" to use the Internet or network connection, you may be breaking many laws including theft of service, unauthorized access to a computer network, criminal trespass, or even federal anti-wiretapping laws.

Now that you have the data, what do you do with it? This section will discuss using a program on the Microsoft Windows platform with NetStumbler data to survey an area. Below, figure 1 shows a sample of data that may resemble the data you will also find. Keep in mind that the percentage of Encrypted Vs. Non-encrypted networks will vary from location to location. In the area where these tests have been conducted, 65.78% of the networks have no encryption scheme implemented. Scary part is the business districts had a higher percentage of vulnerable systems

then residential areas. Another very important thing to look at is the list of SSID names… Many of them are using the default name. Broadband routers with default name will probably still have the default passwords on them as well, and are far more interesting targets then a hidden SSID. Now, back to work…

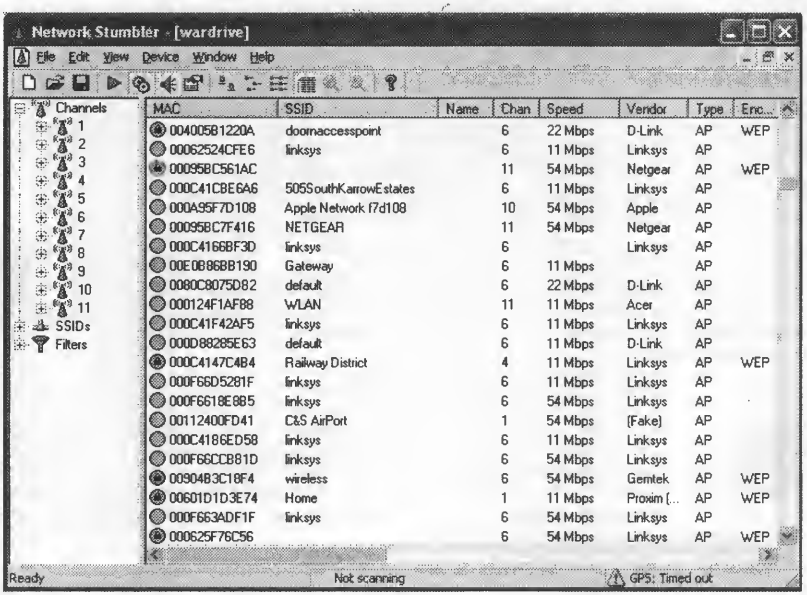


Figure 1 (NetStumbler data gathered during an area scan)

The native NetStumbler file (NS1), can be uploaded to most of the online WiFi public depositories for the rest of the community to view such as wifimaps.com and wigle.net. For example:

Wigle.net quotes Types supported:

- NetStumbler: native (.ns1), text, wiscan, summary
- DStumbler: text output
- Kismet: CSV (.csv), XML (.xml), GPS (.gps), CWGD output
- MacStumbler: plist XML, wiscan format
- Pocket Warrior: Text output

However, if you want to import it into many of the commercial map programs like Microsoft's Streets & Trips or Map Point, you will need to convert the data into a more universally read file such as a CSV formatted file. This is easily done by opening NetStumbler, left clicking on file, Left click on export, and then on Summary. Save the file with a ". CSV" extension and then close NetStumbler. Converting data in general is not that difficult, you just need to be aware of the end format. The exported file is most of the way done, but just needs to go through a little clean up before importing to another program. As illustrated in figures 2 and 2, by opening the file in a basic text editor, you can see how clean the file already is. You will just need to remove a couple lines. If you have programming skills, you can automate the process in very little time.

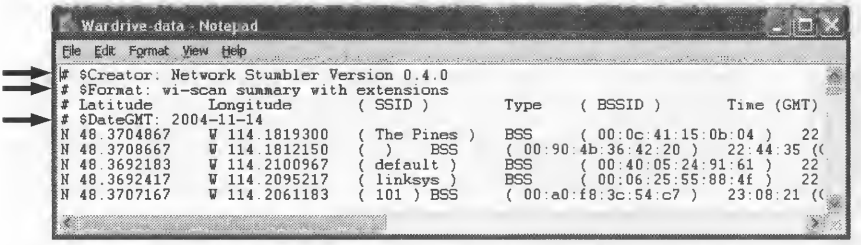


Figure 2 (NetStumbler data export containing proprietary header information)

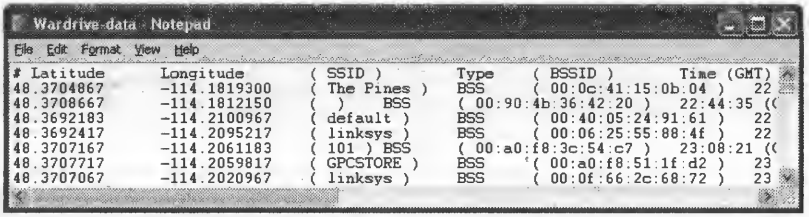


Figure 3 (NetStumbler data export after header information has been cleaned)

Now that you have used Cain, NetStumbler, or Kismet to gather the information, you can start your quest to crack the WEP. The important portion of the data that you will need to start with is the targets SSID, MAC address, and Channel.

Gathering the information

With the needed information, criminals will now start to attack the WEP, or install a Warcracker (small computer designed to automate information gathering and cracking process) that can be either accessed remotely or picked up at a later time. Information Security professionals will sometimes install these devices during a penetration tests or espionage simulations to sniff traffic and archive it for future analysis.

To stay legal while practicing "proof-of-concept", it is a good idea to create a lab environment with several WiFi access points as targets and several systems with WiFi cards to increase the amount of "interesting" traffic. Interesting traffic contains the key negotiation packets and will allow you to gather enough information by sniffing to crack the WEP key in a short period of time. This traffic can be generated by running programs like Aireplay and Void11. This will generate the required WEP initialization vectors for the cracking to take place. Airodump is easy to use and helps with this process.

For this example, the target WiFi Access Point has the SSID of WLAN, MAC address of XX:XX:XX:XX:XX:XX, and the channel of 9. We will use Airodump to capture the weak IV packets and start the passive packet capture to the file named keygen. The command should look like this from the a root level command line shell:

root@home[\]# airodump wlan0 keygen XX:XX:XX:XX:XX:XX

This will save all of the interesting packets in a file called keygen.txt that we will use shortly. However, unless you have a lot of time on your hands, you may want to speed up the process a little. Void11 is a common tool that deauthenticates the wireless clients. This works great in a lab environment, but will set off triggers in a business setting and is a symptom of a possible attack of your system. During a Kismet scan, we have found a client system with the MAC address of YY:YY:YY:YY:YY:YY. This is important because we are going to target that MAC address along with the Wireless Access Point to help generate the information we need. Using Void11, the command should look like this from the a root level command line shell:

root@home[\]# void11_penetration -D -s YY:YY:YY:YY:YY:YY -B XX:XX:XX:XX:XX:XX wlan0

For shorten the time it takes even more, many people use Void11 in conjunction with Aireplay. This program captures valid traffic and replays the traffic and sends it to the Access Point to generate more of the right traffic.

root@home[\]# aireplay -i wlan0 -b XX:XX:XX:XX:XX:XX -m 68 -n 68 -d YY:YY:YY:YY:YY:YY

The entire time the programs Void11 and Aireplay are running, Airodump is capturing packets that will be used in the cryptanalysis process. With multiple systems generating the traffic, a sniffer can record data faster and increase the time it takes to uncover the key. Aerodump can be used to save the traffic to a file, and aircrack can then take that file to attack the key. The whole trick is to force the WiFi device to generate the right traffic.

Cracking the WEP

Now we have a file ready to be sent to the butcher. This is where Aircrack comes in. It will use the Airodump data and start the cracking process to generate the correct key. To break 128 bit WEP, the file will need to have 200,000 to 700,000 unique IV packets. Assuming that we have a good enough file, we attack the file to get the key. Using Aircrack, the command should look like this from the root level command line shell:

root@home[\]# aircrack -f 2 -m XX:XX:XX:XX:XX:XX -n 128 -q 3 keygen.cap*

When the key has been discovered, you should see "KEY FOUND!". At this point, the Wireless Access Point has been compromised and can be accessed. You have now cracked WiFi encryption!

A similar method was use at an ISSA meeting in Los Angeles, a local team of FBI special agents cracked a 128 bit WEP key in three minutes using commonly found tools available off the Internet. This demonstration was done to prove that even WEP 128 is a vulnerable encryption and should no longer be used when securing WiFi hotspots. Keep in mind, the more computers generating interesting packets, the faster you can break the WEP.

In this article, we have discussed the entire process of cracking WEP encryption from the initial search during Wardriving or Warwalking. It is important to become familiar with scanning tools like Cain, Kismet, NetStumbler, and MiniStumbler to help survey the area. The ither tools that have been covered should give you the ability to crack your own WEP key and may now have the extra push you need to convince those with WiFi to move to the next level of security, WPA. WPA or WPA2 encryption is the new commercial standard and is more difficult to break.

- Disclaimer: Do not connect to Wireless networks that you do not have authorization to use. Many businesses are more then happy to share their WiFi signal with you if you are a regular customer. On the other side of the coin, private parties such as home users are usually not as friendly when they see someone parked outside their house in the middle of the night and may call the police. Depending on the laws and regulations in your area, this may be considered illegal. Just remember, Wardriving is the catch and release for geeks. Be safe, be smart, and happy Wardriving.

Resources:

Windows WiFi

- http://www.NetStumbler.com (NetStumbler & MiniStumbler)
- http://www.oxid.it (Cain & Able)

Linux WiFi (Some of these applications have a port to Windows)

- http://freshmeat.net/projects/aircrack (Aircrack, Aireplay, Airodump)
- http://sourceforge.net/projects/airpwn (Airpwn)
- http://sourceforge.net/projects/airsnort (Airsnort)
- http://www.kismetwireless.net/ (Kismet)
- http://wepcrack.sourceforge.net/ (WEPCrack)

WiFi Hotspot online maps

- http://www.wifimaps.com/
- http://wigle.net/

Other good resources

- http://www.cwnp.com (Planet3 Wireless)
- http://www.infosecwriter.com
- http://www.oissg.org (Open Information Systems Security Group)
- http://www.revision3.com (Home of Several Hack/Computer ezines)
- http://www.seattlewireless.net (Seattle Wireless)
- http://www.tomsnetworking.com/Sections-article111-page1.php (FBI Cracks WEP)

UnicOder presents

Cheating on Browser-based Games

A true hacking story

unicoder@blacklisted411.net

Disclaimer: Please do not attempt to recreate any of the things presented in this article. Cheating and hacking websites is an inappropriate and possibly illegal activity. In this case the operators of the website I hacked were aware of the situation and my fake high scores were deleted immediately after the hack.

Preface

Anyone that has ever played browser-based games probably has seen the high score lists with the people on the top with unrealistic scores. You may have wondered: "How did these people manage to get such high scores?" If you were smart enough, you would come to the conclusion that these people didn't play the game for hours just to get a high score, but rather they cheated. But how can one cheat on one of these games? And what can developers of browser-based games do to prevent cheating? This and more will be covered in my article. Prepare for a thrilling true hacking story featuring me – UnicOder - and watch me putting myself on top of a high score list by using some dirty tricks. ;-)

How everything started …

It all started around a month ago, when I was waiting on some of my colleagues at my universities campus. Since they were late, I used the spare time to think about what my next article for Blacklisted!411 would be. Unfortunately I didn't come up with any mind-blowing ideas, so I grabbed my cell phone and started to play Tetris to kill time. I don't remember how long I played, but suddenly I had the idea to write about cheating on browser-based games. I realised that for many years I had wondered how some people managed to cheat on browser-based games, but had never actually tried it myself.

A few weeks later, my vacation started, and I finally had time for some hacking activities. On a rainy day I found myself searching for a website containing JavaScript games on it (I chose JavaScript games for my little "experiment", because most of them suffer from a weaker security than the widespread Flash-based games).
I finally found a website with a bunch of Javascript games on it (Tetris, Snake, Pacman, Minesweeper, …) that seemed worth a hack. I will refer to the website as
www.cooljsgames.com from now on (the original name was changed to protect the page from abuse).

As any ethical hacker would do, I told the operators of the website before attempting to hack the high scores list. Fortunately, they graciously allowed me to perform the hack and later allowed me to publish this article (thanks guys, you are awesome!). This is where my hacking adventure could ultimately start …

Exploring the games on www.cooljsgames.com

Before attempting to do any hacking, I decided to explore www.cooljsgames.com first. I found several nice games and decided to play a few of them. After I finished playing, I decided I would hack the high score list of the Tetris game (primarily because I had the idea for this article while playing Tetris ;-)).

Let's have a look at the Tetris game and how the score submission process works:

First of all you play as long as you can. I guess I don't have to explain the rules of Tetris, as anybody knows this game. When you loose, a "Submit your Score" button appears (*Fig 1*).

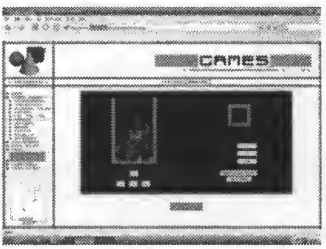


Figure 1

When you click on this "Submit your Score" button, a page showing your score is loaded (*Fig 2*), but the score is not yet entered into the high score list. Before this is done, you have to enter at least a username and a password (which you can choose freely – you don't have to register) and click on another "Submit" button (*Fig 2*).

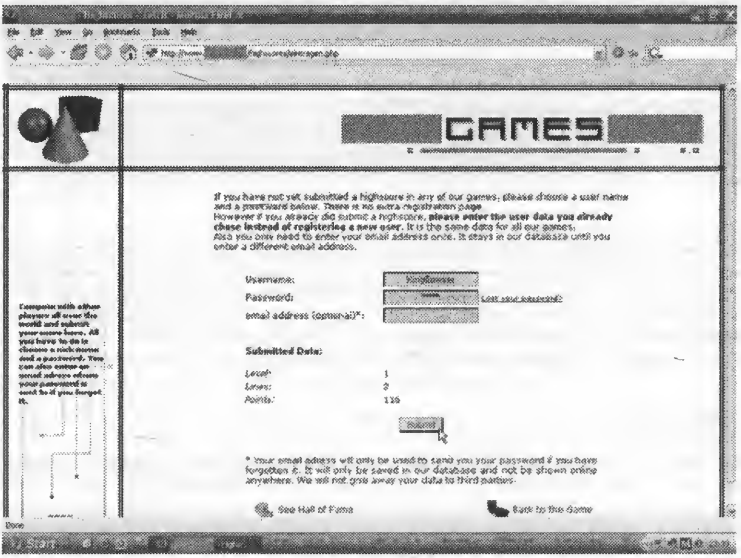


Figure 2

If your computer doesn't drop the connection at this point, a page telling you that your high score was successfully entered shows up (*Fig 3*).

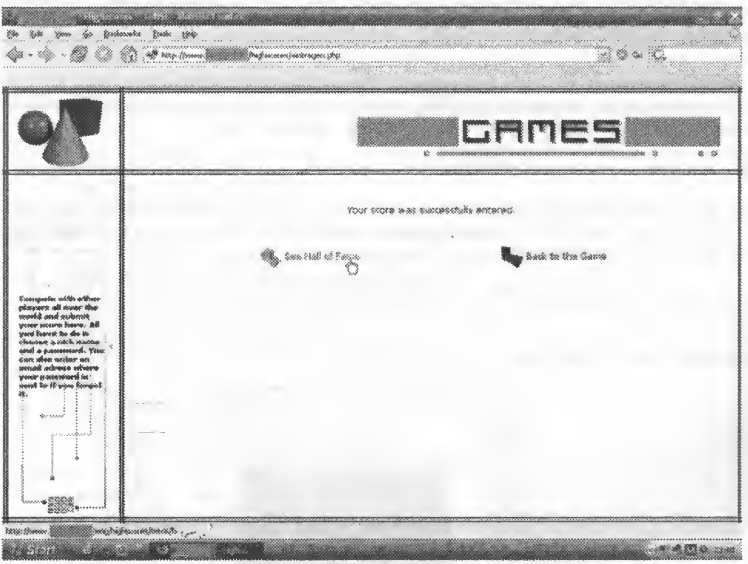


Figure 3

Last but not least you can click on "See Hall of Fame" or try another round of Tetris by clicking on the "Back to the Game" option. When you click on "See Hall of Fame" a page showing the high scores is loaded (*Fig 4*).

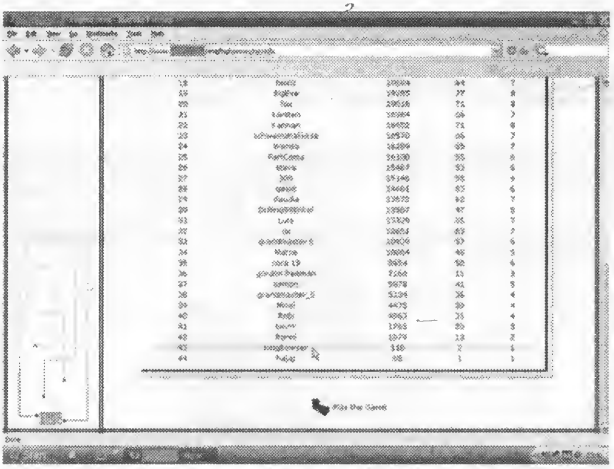


Figure 4

As you can see in *Fig 4* my score was terrible. But this didn't matter since it only gave me more motivation to hack my way to the top.

The first hacking attempt – Modification of the JavaScript Code at runtime …

Now that I knew enough about how the game and the process of the score submission worked, I started my first hacking attempt – the modification of the games JavaScript code. There was one thing I realised outright: The easiest way to place a fake high score into the high score list is to inject the score before it is submitted to the server.

As I mentioned before, the simplest way to boost your high score is the modification of the JavaScript code that is executed on your browser. To carry out this evil plan I decided to try a new extension for the Mozilla Firefox browser called Platypus **[1]**. This allowed me to edit the website (and therefore the embedded JavaScript source code as well) directly in my browser. My intention was to use Platypus to change some lines of the Tetris games JavaScript code (at runtime and directly in the browsers window) to produce higher scores that could be submitted to www.cooljsgames.com later on.

As it turned out, this was not the best plan since Platypus seemed to have problems with the website's massive amount of JavaScript code. Applying the "Modify Target HTML" function in Platypus always resulted in an incomplete presentation of the source code (*Fig 5*). I tried everything but I could not force Platypus to display (and let me edit) the whole code of the JavaScript Tetris game.

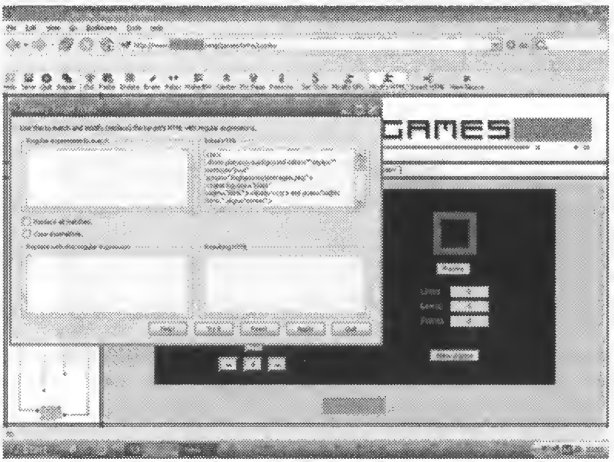


Figure 5

I really don't know exactly why Platypus had this problem – maybe it was because I used a Beta Version (Version 0.51) that is far away from being stable – but I finally rejected Platypus and decided to change the JavaScript source in a good old manner with a simple text editor.

The second attempt – Modification of the JavaScript Code with a simple text editor ...

First of all I downloaded play.htm (this contains the JavaScript source of the Tetris game) from www.cooljsgames.com to my local hard disk and opened the file in my favourite text editor, Programmers Notepad **[2]**. Reading through the code of the JavaScript I found the code passage that dealt with the initialisation of the Tetris game (*Fig 6*).

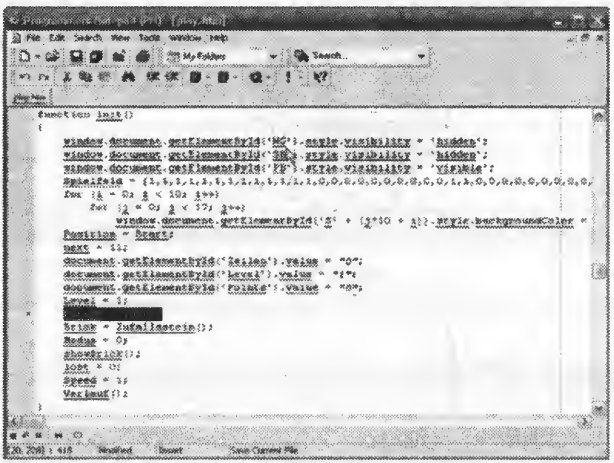


Figure 6

As you can see in *Fig 6* especially one row attracted my attention, because that row is responsible for the initialisation of the points when the first level is loaded (Note: "Punkte" is German and means "Points" in English). Originally the value of Punkte was 0, but I changed it to 10000 which allowed me to start my game right off with a little bonus of 10000 points. ;-) The only other thing I had to do was change the link for the "Submit Score" button in the game, so that it pointed to the online server of www.cooljsgames.com and not to my local hard drive.

After I had made these two little changes I opened the modified play.htm in my browser, and boom - I really started with 10000 points into Level 1 (*Fig 7*).

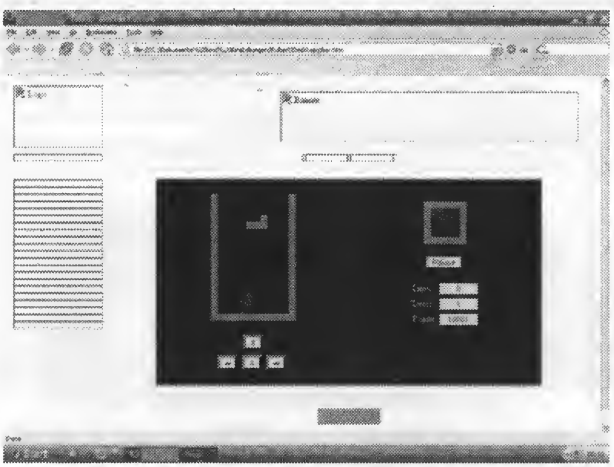


Figure 7

I played on a bit and when the game ended the "Submit Score" button (The link I had modified to point to www.cooljsgames.com) appeared. I clicked on it and thought "well that's it, now my cheated score will be entered into the high score list".

But instead of getting to the screen where I could enter my name and password (see: *Fig 2*) I was redirected right to a strange error page (*Fig 8*).

Figure 8

So what has gone wrong? Thanks to my programming knowledge, I knew the answer immediately: It was very likely that a URL Referrer* protection was responsible for this redirection to an error page without any apparent reason.

What is a URL Referrer? *

The referrer is part of the HTTP [3] request sent by the browser to the web server. When visiting a webpage, the referrer or referring page is the URL of the previous webpage from which a link was followed. More generally, it is the URL of a previous item which led to this request - the referrer for an image, for example, is generally the HTML page on which it is to be displayed. Many web sites log referrers as part of their attempt to track their users. Most web log analysis software can process this information. As referrer information can violate privacy, some browsers have the option of disabling this functionality. Some proxy and firewall software will also block referrers, to avoid leaking the location of non-public websites. This can in turn cause problems: some servers block parts of their site to browsers that don't send the right referrer information, in an attempt to prevent deep linking or unauthorised use of images (known as bandwidth theft).

Parts of the description taken from Wikipedia, the free encyclopaedia

In this case the developers had built in the URL Referrer protection to impede hackers from submitting fake scores (Note: This is a very common method). Simplified such a basic URL Referrer protection to circumvent cheating looks like this:

```
IF referringpage = "correct url"
THEN redirect to submitscorepage
ELSE redirect to errorpage
```

This means that in my case, it was likely that the server of www.cooljsgames.com "saw" that the score was sent from a file that was stored on the local hard disk of my computer, and therefore I was redirected to the error page.

To check if my assumption with the URL Referrer protection was right I downloaded another "HOT" extension for Firefox called Web Developer Extension 0.9.3 [4]. This little piece of software allows disabling the referrer logging among other things.

So I disabled the referrer logging in my browser and played the Tetris game online again. If I could reproduce the

error message with this trick, my assumption about the URL referrer protection on the server was right. And guess what: I got proof that my assumption was right because the same error page appeared. (*Fig 9*) ☺

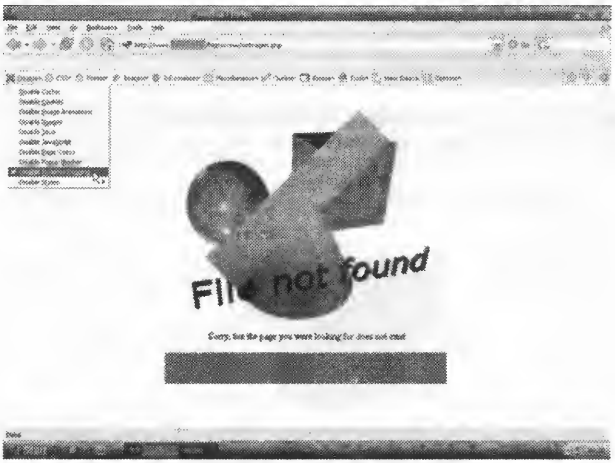


Figure 9

The final attempt – Spoofing the URL referrer / replay attack

To complete my hack, all I had to do was to spoof my URL referrer in some way. After googling a while, I found yet another Firefox extension that was ideal for my needs: LiveHTTPHeaders 0.10 **[5]**.

The LiveHTTPHeaders website says: "This tool is ideal for debugging web applications, seeing which kind of web server the remote site is using and seeing the cookies sent by the remote site." But they forgot to mention one thing: This is the perfect hacker's tool for replay attacks; because this little plugin lets you edit request headers and replay URLs. ;-)

So I played the game again and recorded the outgoing HTTP Header (*Fig 10*), that was used to submit the score to the server (This submission is done immediately after clicking on the "Submit your Score" button in *Fig 1*).

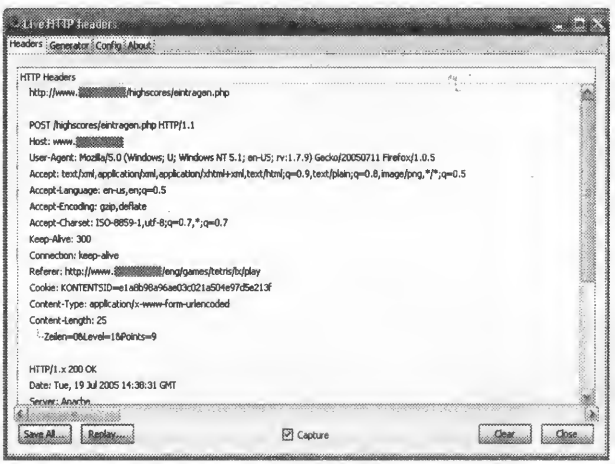


Figure 10

Then the "Enter your Username and Password" page including the submitted score (Zeilen=0, Level=1, Points=9) loaded as usual (*Fig 11*). (Note: Zeilen is German for Rows)

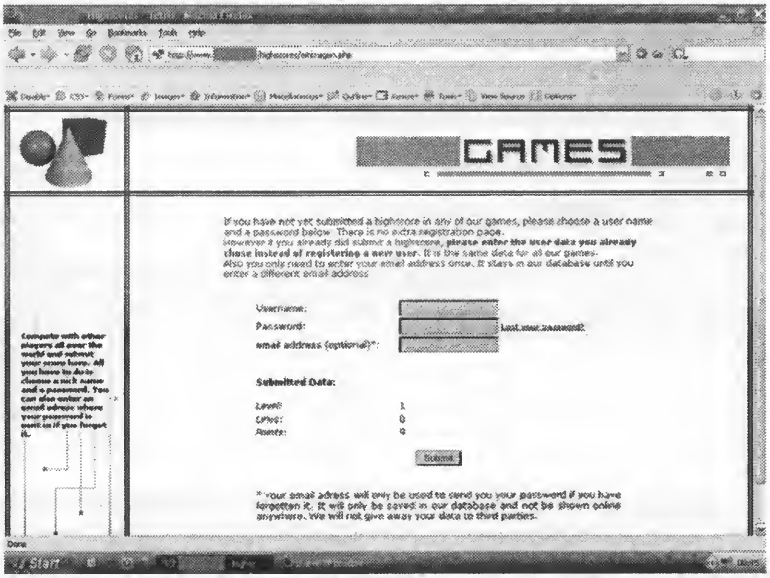


Figure 11

Now it was time to use the replay function of LiveHTTPHeaders. So I pressed the replay button you can see in the capture in *Fig 10* to open the editing window (*Fig 12*).

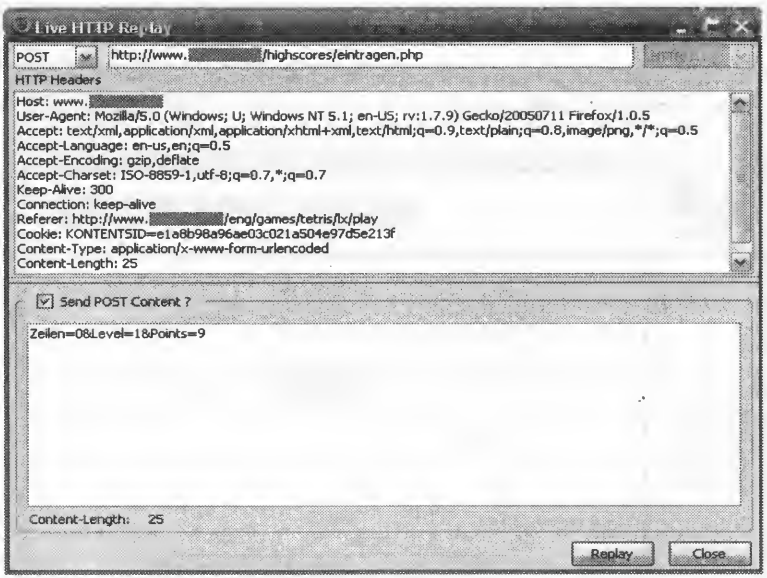


Figure 12

All I had to do now was to change the values of Zeilen, Level and Points. I decided to choose realistic values so that my score would not look like I cheated at first glance. *Fig 13* shows the modified HTTP header. Please note that I had to adapt the content length attribute as well.

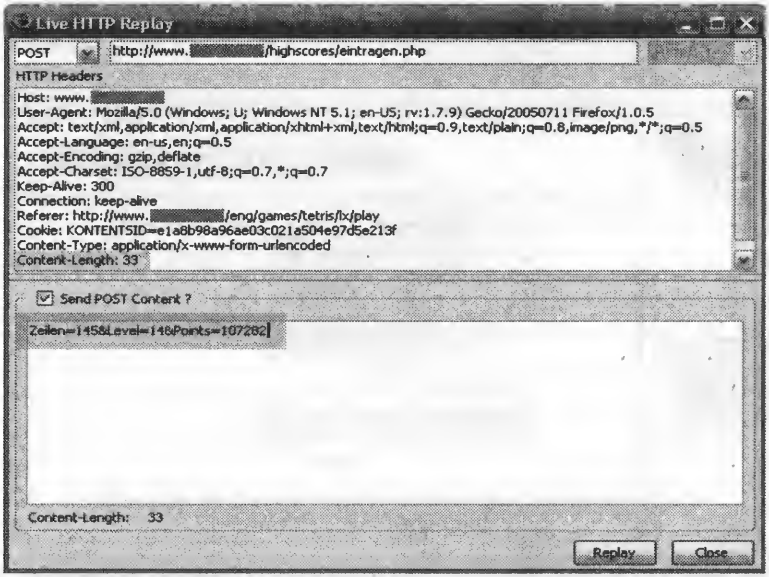


Figure 13

After pressing the Replay button (*Fig 13*) the "Enter your Username and Password" page was displayed, but this time it had my new hacked score (*Fig 14*)! ☺

I was like: "Yea baby, that's it! This is so damn hot!" All I had to do now was to enter my name into the proper field in *Fig 14* and press the "Submit" button.

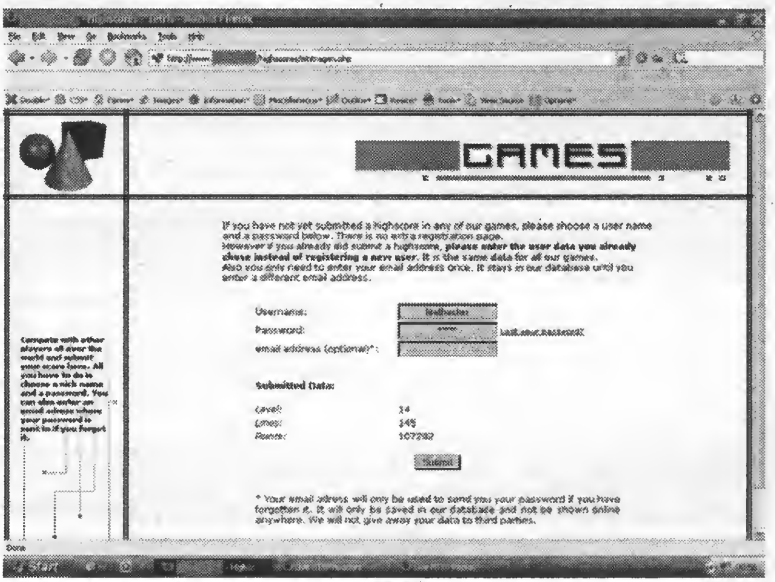


Figure 14

And there it was: Unic0der aka leethacker on top of the Tetris high score list! Thanks to cheating. (*Fig 15*)

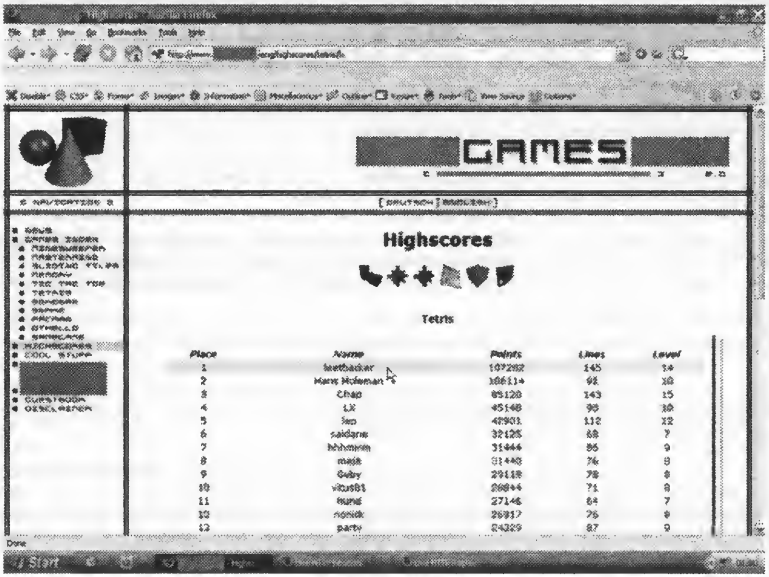


Figure 15

Conclusions

As you can see, there is no magic behind cheating on a browser-based game expecially when the security of the game is weak like the site I hacked. All I needed for this hack was perseverance, a computer with internet access, Mozilla Firefox and some nice browser extensions. But I don't just want to tell you how to cheat on browser-based games, but also how to properly secure them …

3 methods to circumvent cheating:

- URL referrer protection (very basic protection)
- Encryption of the scores sent to the online server (mediocre protection, depends on the encryption algorithm and if its client or server based)
- Additional use of strong session keys (best protection, impedes the replay attack)

The combined use of all three methods mentioned above makes cheating nearly impossible (I do not want to say impossible, because anything can be hacked). All the developers have to do to prevent cheating, is to implement these things into their games. I know, things like encryption or session keys are not easy to implement, but hey – there is no better way to make browser-based games more secure. And what is more important than security?

If you have any further questions regarding this article or if you just want to give me a shout send an email to unicoder@blacklisted411.net, post in the Blacklisted!411 forums (http://www.blacklisted411.net/forums/) or submit a comment to the printed magazine.

And never forget: Hacking is not a game, hacking is survival training. ;-)

Links

[1] Platypus - http://platypus.mozdev.org/
[2] Programmers Notepad - http://www.pnotepad.org/
[3] Hypertext Transfer Protocol HTTP/1.1 - http://www.ietf.org/rfc/rfc2616.txt
[4] Web Developer Extension - http://chrispederick.com/work/firefox/webdeveloper/
[5] LiveHTTPHeaders - http://livehttpheaders.mozdev.org/

Shouts

Ustler and the administrators of the hacked website

FREE BROADBAND

By Dr. Fibes

You're saying "What's that?" Yes, I'm not kidding. No tricks or gimmicks, no salesman will come to your door. I'm going to show you EXACTLY how to get FREE broadband. You're not going to steal it, that's bad karma dude. You're going to use your brain to get it, like any good white hat hacker.

Actually, you're still going to pay for broadband. But you're going to consolidate some other bills into your broadband payment, the net result being your broadband is going to be paid for from this rearrangement. Or at least very close. Perhaps it would be more accurate to say "Broadband for the price of cheap dialup." I think I can safely say that.

Let's do an abridged recap of two-way communication history, certainly not comprehensive.

Once upon a time, personal interaction was the only method of two-way communication possible. If you needed to communicate with someone, you stood face to face with them and spoke to one another. Oh, you could send a proxy messenger in your place, but really, it's about the same thing.

Then that writing thing came along and after a while, many people learned how to do it. Then came the postal service. You could write your thoughts down on some medium and send it to someone far away. After quite a while, you might get a response back from them. It was low-tech to the max, but much better than what was in existence before that time. It got faster and faster with advances in transportation, but there was always a lag in the conversation.

Then the telephone was invented. Amazing. Now you could talk to someone miles away, simply by speaking into this little Bakelite funny looking thing. It sure beat yelling. They could hear you (somewhat) and speak back. You could understand almost everything they said. It helped to revolutionize the world. It was a good thing.

Then along came personal computers. Heck, you could send an email and your contact on the other end would get it almost instantly. Sure beat the snail mail. The "lag" could now be reduced to minutes, even seconds. Even with 1200 baud modems. "Verily" we all said, "this is good." And it was and it is.

But people prefer talking. It's faster for most of them, easier, and the conveyance of information is also superior for most people. You may have noticed that many folks in this world can't spell or write in a very coherent fashion, but most can communicate at least on some level by speaking. And if they are really poor at communicating, at least with voice communication and the inherent instant feedback that occurs with it, sub-standard communication can often be corrected in real time.

We still have Ma Bell, at least a facsimile of it. The price for traditional phone service is somewhat reasonable, although those in the know are aware that it's way overpriced. But not so much so that most people in say, the U.S. and Europe can't cope with it.

But now there's a new kid in town.

Have you heard of VOIP? Of course you have. It's the buzz. VOIP is coming. Soon, almost everyone will dump their landlines and use VOIP instead. That's the popular consensus, is it true? I think so. There are pros and cons to just about everything in life, VOIP is no exception. Let's take a detailed look at VOIP and weigh those factors. And let's try to do it without getting too bogged down in the technical aspects of the subject, but rather from the viewpoint of human beings with human goals and obstacles, seeking ever more effective tools to achieve those goals and overcome the obstacles.

I believe that the main thing holding VOIP back is resistance to change. We've had the familiar phone company system longer than anyone reading this has been alive. We're very familiar with its pros and cons and it does the job. "Better the devil you know..."

Remember dialpad.com? It was one of a handful of companies bringing us this type of technology early on. It was somewhat lame. But it did give a good vision of what was to come. The audio was garbled beyond comprehension at times. You really needed a specialized "operator" type headset (earphones & mike) to use it; otherwise you'd have feedback problems. Both you and your contact on the other end had to have a computer and the Dialpad program installed on them. But it worked OK a good percentage of the time.

When the old Dialpad was in existence, I had many friends in a town about 30 miles away from me. The phone company wanted to charge me $.15/minute to talk to them. This could run into some dough after a month or so of chatting. My friends & I were ecstatic about Dialpad, even with its many shortcomings, because now we paid $0.00/

minute to talk. At the end of the month, we owed ZERO. We'd often talk for hours, why hang up? It was free. Dialpad is now owned by Yahoo. No surprise there, many, many companies are positioning themselves to take advantage of the huge VOIP wave about to wash over the world. That's the real question we should all be asking ourselves: "Whose service do I utilize?"

Vonage is the Verizon offshoot. This is for the sheeple. For those who are afraid of trusting their two-way existence to anything new, Verizon has the answer. At an outrageous price that totally negates one of the most important advantages to VOIP. Those devils…

Redundancy is also an important issue. Any good engineer will design in some degree of redundancy if at all possible. For an often quoted example, the shuttle has 3 computers that "vote" on every decision. Another example: all cars since the 1960's, perhaps even before, have separate hydraulic systems for the front and rear brakes. If one fails, you still have at least some braking power in the other. Communications can be vitally important, if we desperately need to communicate, we want to be sure that we can.

Let's go back to our once upon a time scenario. Not that long ago, the ONLY method of two-way communication was the telephone. Now most of us have: email, landline phone, cell phone, chat services, etc. Even the lowly phone booth counts unless you live in the woods. That's a lot of redundancy.

Just how much redundancy do you need? Near as 15-20 years ago, most folks had only the telephone and the phone booth. Ok, that's two methods of two-way communication. Now let's add in today's cell phones and the various internet services. That's four methods in the modern world (counting the myriad of internet services as only one system). How many backup systems do you really need?

IMHO, the cell phone is a viable backup service. Excluding the phone, phone booth and cell phone, all of the communications I have mentioned utilize the internet in some fashion. Perhaps then some are concerned with the question "What if my ISP goes down?"

Well how about this. Let's say you live somewhere and a big disaster occurs, maybe a huge hurricane. Hey, that just happened. Did Ma Bell's communications system survive? Nope. Pretty much nothing did. So what did those poor souls gain from the redundancy of the phone company?

Yeah, your ISP may go down. The phone company may shut down. The cell relay satellites may get fried in the blink of an eye. That's why we have redundancy.

What I am speaking of is this: with your ISP, cell phone and the same old lowly phone booth, you already have multiple options, more than you had 15-20 years ago. Do you need another one? Some may answer "Yes." Then plunk down your $30 + per month and you shall have it.

For those that feel three options are reasonable, call Ma Bell and tell them to take a hike. You just saved $30 + per month. What's that broadband cost? Huh, about $30-35 per month. Now we have come full circle to the point of this article.

In a case like Katrina, about the only things that would have kept you communicating with the outside world would have been a battery-powered ham transceiver and a good antenna. And then only if you had been able to keep it from getting soaked. In most of the stories you read, those poor people said it happened so fast all they had time to do was head for the attic. It's not likely anyone would have had time to grab the transceiver from the garage, much less the antenna. OK, maybe a two-meter handheld could be handy.

The point is: how many of you landline phone fans have a ham transceiver in the garage? If you're truly serious about having as many options as possible come hell or tsunami, shouldn't you get one of those too? It just doesn't add up.

Now VOIP isn't free, at least convenient VOIP. So you've got me, you may not get off quite free. But darn close. If you take an HONEST look at your phone usage you're likely to find you can get what you need in a VOIP service for less than half of what your Verizon or other traditional phone service charges monthly. With no change whatsoever in your usage habits. Isn't that a good deal?

Incidentally, if you paid attention to the news, the people interested in pushing WIMAX were down there in New Orleans before any other communications industry, providing WIMAX VOIP to the survivors. Ma Bell was nowhere in sight. How's that for a testimonial?

Many are probably dragging their feet about VOIP due to equipment cost. While VOIP offers vastly superior audio quality in comparison to standard phone lines, unless you replace your phones with VOIP enabled phones, you won't notice much improvement, although even if you don't you'll probably notice some. Last I checked VOIP phones were pretty pricey. For you shoestring people (like me) using your current phones is a good option. Yeah, it won't sound like an audiophile stereo system, but it'll be at least as good as what you're used to and much cheaper.

Then the only equipment you'll need (because you're already going to get a router for your broadband, right?) is a VOIP to RJ-11 adapter. I just checked on Ebay, they're going for between $15-99, with shipping. In most cases, you'll just DISCONNECT YOUR EXISTING WIRES TO THE PHONE COMPANY, plug the adapter into one of your existing phone jacks, hook an Ethernet cable into your router and then start calling people. No heavy duty phone wiring exercises. The same wires that already exist in your abode will suffice.

IMPORTANT NOTE: Follow the manufacturer's directions, not mine. This general description is not meant to be an instruction manual on installing a VOIP adapter. You assume all risk even if these instructions are wrong, etc. etc. Specifically, you'll blow your new adapter if you don't disconnect the service lines from the phone company before doing anything else.

The available plans by providers vary greatly in this infant industry. And what suits me may not be right for you, so I'll leave that for you to do on your own.

The services offered vary greatly as well. Some have 911 & 411 service, others don't. Most that don't say they'll offer that in the future. But most providers offer things like call forwarding, caller ID with name, call waiting, distinctive ring, voicemail and others STANDARD. Add those up on your traditional service.

Some allow you to transfer your existing number over, others don't. At least one utilizes your computer bandwidth to conduit their business in exchange for a low monthly rate, the majority of them don't. Most allow you to use your laptop as a cell phone in Wi-Fi hotspots. It goes on & on, you'll just have to decide which factors are important to you.

Be sure and snoop around to see what actual customers of that provider have to say about their service. I haven't seen too many negative comments, but better to find out before you plunk down your bucks.

A few, like Vonage, require that you use THEIR adapter. Check out these details with a potential vendor before getting that whiz-bang adapter on Ebay.

You may have noticed that I haven't spoken a great deal about the technical aspects of VOIP. That's because it's really not necessary to go into that to get a grasp of the possibilities here. It's what you're already used to with phone service. Sign up, plug it in and start talking.

After Katrina, Rita came rolling in from the Gulf to hit Houston. Many Houston residents, with Katrina's awesome horror still fresh in their minds, hopped in their vehicles and headed north. The traffic jams were tremendous. Fuel ran out at the gas stations along the way. It was yet another nightmare.

Yet if these folks had thought about it for a few minutes before they left, they would have realized that this would be the case. Why not head to the west or east to a road less traveled? They had plenty of time, they could have even made it to high and dry Arizona before Rita made landfall.

Follow your heart, not the herd. They'll follow along shortly in this case. If you're on dialup, trade it in for broadband now for the same price or less. If you're on broadband already, start saving now.

And my apologies to the people of Houston, hindsight *is* 20/20. After Katrina, who'd be criticized for not running like crazy in the opposite direction? The analogy was for the purpose of illustration only.

How would I hack thee?

Social Engineering and the Basic Hack

By M L Shannon

As we all know, there are many sources of information, but some of which are not so easily accessable. So when someone has good reason to obtain this information, but are prevented from doing so, then what might be called extraordinary measures are called for.

(Insert theme from Mission Impossible here)

This could mean physically entering the facility, the place where the files are stored, which might require resorting to something as ham-fisted as breaking down a door, (which you are aware if you have ever done it, makes a great deal of noise, often sufficient to wake up the midnight shift IT people) or with a bit more finess (like the geeks in the contest at DEFCON 13) lockpicking.

But sometimes, Oh Joy! it is possible to hack ones way into the repository, or even better, depending on particulars, find someone else to do the job.

Now, in such a Black Bag operation, a good way to begin is to make a plan, calculate the odds. The chances of success compared to a free ride in a foul smelling van full of nasty criminals all wearing designer stainless steel bracelets by Smith and Wesson. Not to mention the loss of your laptop.

Case the Joint

Over the years that I have been involved in electronic surveillance and countermeasures, it has become second nature to wonder, when I enter a room, how someone would go about installing listening devices. How and where. I learned to think that way, a mindset that is necessary when working a TSCM sweep.

Now, one criteria (TSCM techs use that word sometimes, just as the old timers still say 'clandestine') is the possibility of an inside job.

Devise a plan. Check the perimeter, and if possible get inside and have a look. Take stock of the tools available for the mission and . Devising a plan and all that. fix

In my earliest experiences searching for monitoring devices, there were few personal computers and most businesses didn't even have them. But the TSCM technician today has to deal with computer systems as they are present in most homes and virtually all businesses.

So, along with opening all of the books on the shelves and removing plastic plates from wall plugs and switches, peeking underneath desks and tables, it has become necessary to test clients systems for vulnerabilities. Such as machines that do not require a username and password to access them, passwords that are easily guessed or written on a Post-It and stuck on the back of the monitor or in an unlocked desk drawer, and worse, terminals left online, the user not having logged out. On one sweep, which was a large corporation that you have probably heard of, I found a number of them.

In the wireless world, we now look for Access Points that don't use at least WEP and are sitting in front of a window, and of course "rogue" wireless Access Points installed by a competitor's spy or unhappy employee about to quit.

But I had always approached this from a countermeasures perspective; on the defensive, wondering how someone else might attack a system, and how I might discover what they had done, rather than how I would go about it. They are much the same, but not entirely.

That was until something happened to change the way I looked at one system in particular, and wonder how it might be possible to hack my way into it. For a reason that I believed was justified. Should you have read my first book, Don't Bug Me from Paladin Press, you might recall where I stated that while spying on someone without them knowing about it is legally wrong, it is not necessarily morally wrong.

In that book, I tell the story of a beautiful young girl that was being stalked and terrorized by her ex-husband and no one could do anything to help her. Until, that is, an electronic technician bugged the guys bedroom and got the goods on him. Confronted with the evidence - tape recordings- he never bothered her again.

Sometimes spying is justified, even if it is unlawful.

Many years later something happened, a problem, and though it was later resolved, at the time caused me to start thinking about how I might take care of it myself. I had what I believed to be morally justified reason to access information as I will describe in this short article.

I was waiting in the examining room at a local clinic. The doctor comes in, a puzzled expression on his face. Now that alone was enough to freak me out and when he sits down and says he "has something to discuss with me", my pulse rate goes into triple digits.

He wants to know about a problem I supposedly had relating to one of the other physicians there, which was a mystery to me- I had gotten along fine with everyone there. At least as far as I knew. Then he asked if I had been examined for (a serious disease) recently, that there was a note in my file about it.

I am starting to wonder if he has the right file and he verifies this, so I want to know what the hell is going on. But he won't tell me anything. Covering up a mistake? I wonder.

After the exam I ask if they can fax me a copy of the blood test result and am told no. No way. I will have to make an appointment (which takes several weeks) or come to the urgent care clinic which means sitting in the lobby for several hours and taking up staff time that could be used for someone really sick.

This clinic is part of the City and County Health Department network. It links the many satellite clinics, hospitals and other facilities and stores information on the patients that visit them. So, what if I wanted to look at my own records, to find out what the hell they didn't want to tell me. Or maybe even someone else's file?

And, again, while the information was soon made available to me (and there were no physical problems requiring treatment) still I wondered, how might I go about getting into the system?

Social Engineering 101

Now, this particular facility was open to patients on a sliding-scale basis, a place for low income people as well as starving writers, and at the time I qualified as I had no steady income. It was also for the homeless, and so, the 'average' patient might be assumed, by the health care workers, to not have much in the way of computer skills.

At least that's the impression I got when I started probing for answers. Playing dumb, of course which is an important factor in social engineering.

In many, if not most situations, give the person you are quizzing the idea that they know much more than you do and you'll get more answers than if you come on with a lot of arrogance. Although sometimes you need to come on a bit heavy as you will read later on.

I scheduled a visit, having had a minor foot injury and complaining of back pain, which was real and probably the result of sitting in front of this damned monitor so many hours a day. I get there, get signed in, the usual temperature and blood pressure check and "Do you use drugs? Yes. What kind? Heineken. Is that all? Yes."

After waiting a couple hours, trying to read a book on the Linux operating system that is mostly g(r)eek to me, I am led to an examining room. The nurse comes to ask the requisite, 'where does it hurt' questions.

While I am explaining that my foot hurts (it really did since I dropped a power supply on it) and that I have upper back pain (I don't mention computers) I stare at the terminal sitting on a shelf and work in a few innocuous questions. Like whether or not 'that computer' had Donkey Kong and if they could send that "Internet Email I have heard about". She didn't know if it was connected to the Internet but yes, they could send mail to others on the "circuit". The Donkey Kong question was ignored but I suspect it served to make me seem ignorant as well as harmless.

"Hey, wow, that's neat - you can call up the computer when you are at home to check up on patients and stuff, eh"? I was referring to RAS but again, of course I didn't use the term.

She didn't know for sure but said she assumed that The Doctors would, like for emergencies, be able to. So, it appears that the network does have RAS.

I let it go at that.

The nurse leaves and again, I wait for the doctor. I am tempted to try punching a few keys but decide to wait and try to get more information. I do look at the back of the terminal. Two USB ports. Cables are power, monitor, mouse, keyboard and a CAT-5. But no RJ-11 phone cable.

The Doctor comes in, asks me questions. I explain about the injury and some other symptoms and that I think I have plantar fascitis. He looks at me with a quizzical expression and I tell him that a friend I was visiting looked on the Internet after I mentioned my foot problem, and he found this place that told all about it.

So I asked, maybe you can find that place on this (I point) computer?

He doesn't know.

Doc leaves telling me nurse will be back with my prescription in a little while.

I still resist temptation I don't touch the terminal but I am thinking. Plotting. Mentally hacking.

Making Plans
Now, how am I gonna get into this system?

I want to be prepared, so I consider all my options.

If the terminal is active, and runs off a Windows server, I could maybe plug in a thumb drive and if it uses Plug and Play, the drive will automatically be assigned a logical drive letter. But if it is a Unix system, I am out of luck as I don't know Unix well enough to get the thing mounted, which would probably require root or SU. In any case, his has to be done fast to avoid having to explain what I was up to. And keep in mind that we live in the post-9-11 America. Such an attempted hack could very well mean getting busted. Handcuffs. Jail, even.

I could install a key logger in the keyboard cable, then power down the terminal so that the next person to use it would have to reboot it and enter the info I want- user ID and password.

I would need to be able to get back into the same examining room to retrieve it, but this is no big deal. I wait two days, go in, have a seat in the waiting area across from that exam room, and wait till it is vacant. I go in and if anyone asks what I am doing there, I say I lost a ring last time and was looking for it. They buy it and ask me to leave. But it took only ten seconds to retrieve the keylogger.

When I get home, I see what is on it. With a little luck, a user name and password. Maybe links to other networks I can make a note of for future reference. Whatever.

The Internet?
I already knew they have Email on their net. And the doctor who gave me his card has his Email address on it. David Barnyard MD. daveb@healthiernet.org.

So, their network can be accessed through the Internet. At least their mail server. Time to dig around. I fire up NetDemon, (from www.netdemon.net) an excellent suite of IP tools.

First, I check the IP. Enter healthiernet.org and I get the IP which is `204.XX.XXX.X`. To make sure it is up and running, I ping it and get

```
reply from [ 204.XX.XXX.X]   172 ms
reply from [ 204.XX.XXX.X]   188 ms
reply from [ 204.XX.XXX.X]   187 ms
reply from [ 204.XX.XXX.X]   188 ms
reply from [ 204.XX.XXX.X]   172 ms
--- ping statistics for 204.XX.XXX.X
    5 packets transmitted, 5 received
    round-trip time (ms) min 172, avg 181, max 188
```

I could run traceroute but it isn't necessary as I know the network in here in the city where I am. But I do want to see if Dr. Barnyard's Email address is valid, so again I use Net Demon. It is a valid address.

Then, I do a Whois on healthiernet.org.

```
OrgName:    City & County of West Woogieboogie
OrgID:      xxxxxxx
Address:    XXX Networks, Department of xxxx xxxxx, 1234 Kowabunga Street, 3rd
Floor
City:    West Woogieboogie
StateProv:  CA
PostalCode: 94103
Country:    US

TechHandle: BH267-ARIN
TechName:   Jones, Bob
TechPhone:  +1-415-255-xxxx
TechEmail:  bjonez@healthiernet.org
```

Now I know where they are located, and I have a contact name. Maybe Mr. Jones will be useful if I approach him the right way.

Next, I type the IP into Firefox and check out their web site. Much useful information here- names of people I might get answers from. And I examine the source. Hmmm. I see the webmaster's name and Email and that it was built using Front Page. I make a mental note of that.

Wireless?
So far I haven't seen any wireless equipment anywhere in the clinic, and my little keychain WiFi detector called The Seeker hasn't indicated the presence of 802.11 but that doesn't mean there isn't any.

The clinic is in the same building with several government offices, so maybe there is an AP somewhere inside one of the private clinic areas that connects to one of these offices. For whatever reason. And some of the clinic terminals might be on a segment that feeds through the router and into an AP.

So next, I might try camping out on the street across from the clinic.

To avoid drawing suspicion, I go to Goodwill and get a used messenger bag and a clipboard and take one of my radios. Like mail delivery persons, messengers are 'invisible; no one pays any attention to them.

With a Zaurus running Kismet I will capture anything within range, and of course it will look like I am a bored delivery person waiting for the next pickup and playing with something like a Game Boy. (Messengers are computer illiterate. Everyone knows...". Comment heard in an elevator).

Another lesson in Social Engineering. Don't attract attention. Look as if you belong where you are.

Port Scanning
I have their Net Range from whois, so I could look for open ports, but this would be only if all else fails. Even with budget cuts and staff shortages, they still have IT people to keep such an important net up and running. There too much of a chance of getting nailed (door kicked in, Homeland Security people with machine guns, etc.) unless I can work without being traced.

So, at least for now, scanning is out.

The Old Geek in the Maintenance Man's Coveralls Trick

Here is where another version of social engineering is appropriate

Having made a few queries to the doctors and nurses, I had come to the conclusion that they are generally as computer illiterate as they think their patients are.

And being as busy as they are, they don't have a lot of time to deal with things other than their patients.

The Operation
I have decided on the keystroke logger. I install and retrieve it as described, and I have lucked out. I have the login info for three different staff members including one doctor. The same one that gave me his card a while back.

There is an Internet Cafe down the street from my apartment that I can connect to for free. The owners don't know this- the people who go there don't either. They pay six bucks an hour for access to the desktop machines.

Another possibility is to use dial-up from someone else's phone line if one is available.

In either case I would use my DEC 'sterile' notebook computer. The hard drive has been formatted and wiped and reformatted, has never been online, and no software is used that could be traced back to me.

Overkill? Why take chances?

And, of course, I don't want to alert anyone that I am trying to get into their net.

So, at this point I have login info, passwords, but no access. If I were left alone in one of the examining rooms long enough, then maybe I could find the data I want but this is improbable, what with so many staff people in and out, and who would definitely want to know what the hell I was doing messing with one of their computers.

"Uh, I thought the nurse said you do have Donkey Kong."

Not the best of plans.

But remember that the network does have RAS. So what I need is a phone number.

I call the number I have for their network facility on 1234 Kowabunga Street and, in my best German accent, request to be connected to "the person in charge".

"This is Dr. Sergut Braunschweiger with the XX General Hospital's visiting benign hyperparapatuitary hematology analysis group. You are aware that we would be here, are you not?"

Now this is where arrogance can be useful in Social Engineering. You are a physician to begin with and by hitting the poor IT guy with something, bullshit medical terminology that he probably wouldn't understand even if it was real, and in any case, that sounds important. So, you have him on the defensive.

Look, I was given a wrong number to connect to the database for hematology patients records that are part of our study and I need to get some case file numbers for my presentation.

I was told to use 255-xxxx

Since you, as the doctor, have the right prefix, the IT guy is more likely to five you the rest of the number. Once you have that, use a Terminal Emulator and connect. Use the login ID from the keystroke logger and you are into the network.

Conclusion

So how did I finally get the files I wanted?

Not by hacking into the network. I used yet another variation of social engineering.

Hospitals are, to repeat myself, very busy places with doctors and nurses, orderlies and security guards, confused patients and concerned visitors running round.

Again, looking like you belong where you are is imperative. Next is knowing the language, the terminology, and of course knowing where the information is located.

Next, what are you likely to see lying around in a large hospital?

Uniforms. Whites, greens... and here and there, the unquestioned badge of authenticity, the stethoscope.

I have 'the patients' (my own) ID card and so the required numbers.

So I take the elevator to the third floor. Medical Records.

"Patient Shannon is in ER on a gunshot wound C and B claiming has B neg and I need his most recent blood workup stat."

A few minutes later, I have my own file. And a small digital camera.

Hacking is only part of the process of obtaining 'forbidden' information. Social Engineering will often produce results where super-geeks might fail. And that, getting the information, is what it is all about.

Oh, I left the stethoscope behind; I didn't steal it.

The Hacker Chronicles

An accounting of the life and events of a real honest to goodness old school hacker.

PART V

**** A series of articles written exclusively for Blacklisted! 411 ****

By Cactus Jack

Inspired by the recent re-discovery of Blacklisted! 411 magazine and at the request of my wife, I've agreed to write a quasi-autobiography of some of the goings on in my life that relate to hacking <both directly and indirectly>, from as far back as I can recall. Amazingly enough, I recall everything from the time I was a few months old up until right now, thirty some odd years later. Very few people have a memory like mine, but those who do should use their gift to teach, instruct and entertain others. If anything, simply detailing experiences and providing a lesson in history would be more than adequate in helping the cause. With this in mind, I intend to detail as much of my life as possible, noting the many hacker related experiences I've had. I hope you enjoy the read.

Welcome to the fifth installment of my ongoing article.

The Post-College Years

To bring you up to speed in the story, I had just finished college, had a bank account full of money and decided to take a long break from work. I was completely out of the loop for two years, in fact. As far as I was concerned, it was a long needed (and deserved) vacation to say the least. Sure, I was still interested in technology and continued to upgrade my machines as time passed, but I didn't really explore hacking during that time. I just focused on buying up pre-made gadgets and didn't bother dissecting them or constructing anything new.

Anyhow, after just over two years of practicing being a lazy bum, I snapped out of it and dove right back into life, head first. Hacking was my first priority. The year was 1992. The first thing on my agenda was to get out there and buy up some electronics surplus to bulk up my own hacking supplies. First stop was Barry's (ECSC). As Zachary Blackstone has suggested since his first issue of his disk based hacker magazine in 1983 (yes, I was an avid reader of his disk magazine back in the day) Barry Gott was extremely easy to deal with and it was nearly impossible to leave his store without buying a truckload at a time. I bought so much good stuff on that single trip: RAM, EPROMs, programmers, test gear, wire, blank copper-clad circuit boards and a couple of payphones. Next stop were a couple of lesser known salvage yards that happened to cater toward electronic/computer scrap.

By the time I had finished stocking up, I was prepped and ready to dive right into hacking again. I started by focusing on my old Amiga. Years earlier, I had helped design the platform for a multi-serial card that later evolved into the Comports 8-port high speed serial board. With that in mind, I decided to try my hand at designing a new 32-port card capable of running all high speed modems. Within two months, I had a prototype board running. I handed the prototype over to Zach at Blacklisted 411 Magazine and they used it for their online BBS up until the day they pulled the plug. I eventually sold the design and prototype #2 to DKB but they never did anything with it to my knowledge. You see, the Amiga was kind of on the way out at the time, so a lot of companies stopped dumping money into the production of new hardware for it. Too bad, it was a nice machine. Regardless of this, I kept working on Amiga hardware and sold one-off's as much as possible.

After playing with the Amiga for awhile and listening to music on it, I tried my hand at programming a SID player—remember the old SID songs? Anyhow, it was successful and I then had to dig up my old commodore 64 diskettes to try and get my massive collection of SID songs. Ok, found the disks, but had no way to move them from the C=64 disks to my Amiga. Hmm. So I had to design a conversion process of some sort. Eventually, it turned into a cable/interface/software package that allowed me to connect a 1541 (or 1571) disk drive to my Amiga. Ok, problem solved. I enjoyed my SID songs to no end.

In fact, I enjoyed them so much, I decided to hack the (6581) SID chip some more. I did it awhile back and then left the c=64 "scene"... I had to gut 5 or 6 C=64's to get the SID chips I needed to start designing something. Let me tell you something about this chip. Not only does it have an amazing sound, it's also VERY easy to work with. The signal to noise ratio isn't that great, but the unique sound it produces has probably introduced more people to hacking than anything else. The end result of my 6581 hacking netted me a working stand-alone SID keyboard and a working SID MIDI box. I still have my SID MIDI box to this day (2005) and use it from time to time. As for the keyboard, it was sold to someone in the Netherlands in 1994. Never saw it again. I know, so sad.

Oh yeah, during this whole time, I forgot to mention where I was working. I picked up a part time job with a local custom circuit fabrication plant (actually, it's a pretty well known firm). Whenever a customer would come in needing a special something or other, I'd pick up a job to design it for them. It was extremely good pay and the part time status allowed me the freedom to work on my own projects on the side. I used their facilities to manufacture my own stuff and they had no problem with it—was one of the best perks of working there. I could fab a circuit board in minutes on their equipment.

Eventually, all this designing lead me to arcade games. I used to be so into arcade games back in the 80's, I couldn't help but notice when the games started popping up in surplus circles and, eventually, in the auctions. Back then (1993-1995), you

could pick up rare classics (Atari Quantum, Williams Inferno) for $100 or so. Naturally, me being the pack rat that I am, I gobbled up dozens of games and stored them at my place. I immediately began diagnosing dead games and quickly discovered that they were rather easy to work on. I also noted the number of "custom" chips a lot of these games required. The first game I tackled was an Atari Star Wars cockpit version. The board was dead, the monitor was dead, the machine itself was in EXCELLENT condition. The monitor took me 15 minutes to repair by replacing all the transistors on the chassis. Did the trick and it fired up immediately. I had a spare board, so I was able to test it. However, I still wanted to work on the original, because it was upgraded to an Empire Strikes Back.

The first thing I noticed was the ESB daughter card and the small custom chip attached to it. Luckily, the part was still available through a couple of sources at the time, so I grabbed up a few of them. Next thing I noticed was a custom chip by the number of 137179-001 (I still remember it!!) I was able to buy up a small lot of 50 of these from a local repair shop. They had no idea what they were, but they had a bunch. I got the entire lot for $10. What a steal! Anyhow, I was able to repair the board with little time invested. It turned out to be a bad EPROM on the CPU board. I had an extensive collection of programming equipment on hand, so it was an easy fix. Anyhow, this game repair was the one that got me into arcade games with both feet. I realized that these custom chips would run out at some point and people would need them. Perfect situation for me since I loved reverse engineering.

I started picking up side repair work from a dozen different repair shops around the area - yeah, there were a lot of them still around back then. I had a reputation for being able to repair the "tough" ones and the multi-board setups. I have to admit, I was fast, accurate and inexpensive, which is why I was able to pick up so much extra work!

Several things I contributed to the "community" during my days of hacking arcade games:

1. I provided alternatives to custom chips for Atari, Williams and Bally/Midway boards. Specifically, I was able to produce a discreet component version of the 137179-001 chip that Atari used on several of their boards. If you look around, you can find the plans for this floating around the net even today. I also provided alternatives to the customs on the Pac Man/Ms. Pac Man boards. I see that many people have duplicated this effort over the years. That's cool to see that there are still some active hardware hackers among us. I also produced an alternative to the custom chip used on the Empire Strikes Back upgrade, allowing anyone to make the upgrade themselves.

2. I compiled a log of known good EPROM and PROM checksums for hundreds of games, mostly keeping to Atari, Williams and Bally/Midway. What was great about this log was that I included checksums for what has become some of the rarest of the rare games ever produced. When I got started, there wasn't much demand for these, so it was difficult to tell what was "rare" and what wasn't. If I had known, I probably would have kept a few games. I released this log to so many people over the years, I know it's out there on the net now. I have not done a search for it, but I know that work was put to good use by a lot of people so it's proliferation into the net is all but guaranteed.

3. I started a GAME-to-JAMMA standard. Personally, I hated JAMMA games more or less, but it sure made it easy to work on games based on a single test rig capable of plugging any game into. Eventually, I started making conversion harnesses to allow easy hook up into my JAMMA rig. Until then, I had a special rig for each game I worked on. I even produced a small portable JAMMA test rig that could be dragged on location to work on games outside the shop. I built 25 of these for a local repair shop as part of an exclusive deal. I just saw one of these sell on ebay a few months ago. It went for $800-ish. Not bad!

4. I created a repair log for each game I worked on. Most of these logs ended up being about an inch thick with paper. I included notes, checksums, symptoms, diagnosis, parts alternatives, etc. I had planned on taking these logs and turning them into repair books, but I never got around to it. I did release notes as people required them, helping people fix their own games. However, I still retain the entirety of my repair logs and intend to send them off to a publisher eventually. I figure since most of these games are now classics, people can really benefit from my vast knowledge of the repair of these machines.

Needless to say, I enjoyed the arcade hacking to no end. I finally got out of it because I had done so much and it seemed that the few arcade companies I worked for were starting to do so badly (as far as income) that it wasn't worth it anymore. All but two of those companies have since gone out of business, making it even more desirable to get back into the arcade repairs again. Who knows, maybe I will someday.

My experience working on arcade games landed me my next job. I started doing contract work, designing devices for a large company still in business today. (By the way, I'm purposely leaving out names so I don't piss off any of my past or present employers.) They in-turn sell these designs to their clients who manufacture the devices and put them on the market. Many of the little electronic gadgets you guys play with today, I've probably played some role in it's design somewhere along the way. I've done everything from telecommunications and satellite to radio controlled and home A/V equipment.

I started out as a curious kid, interested in what made things tick. Now, I'm helping to make the things that tick. How's that for full circle? Hopefully, there are some out there who pick these things apart and will eventually take my place as a designer of technology. I'm getting to the point where I'm thinking about early retirement, so all you hardware hackers out there, be advised, there are cool jobs waiting for you in the technology sector. My job may be up for grabs sometime soon. I'd like to see a fellow hacker get the job.

Now I'm going to go on a small rant. Who are these people who keep saying hackers are bad? The media, law enforcement. Those are the two main offenders. I'm a hacker. I'm a GOOD hacker. I create and build new technology. I'm the one responsible for making those very tools and gadgets the media and law enforcement utilized to do their jobs. Talk about ungrateful? Why don't you guys smarten up a little bit and take out your aggression on real criminals. I can't understand when being curious became synonymous with being a criminal. It aggravates me to no end when I read the headlines. It saddens me that the once proud name of "hacker" has been trashed over and over again by these two entities that the general public now thinks hackers are bad people. However, I have noticed a trend lately, following the Matrix movies, that people generally think that hackers are "cool" and mysterious. I suppose I can live with that label. Hey, it's better than the alternative, right? Anyhow, with this said, I conclude my series. I sincerely hope that some of you found my stories to be of some interest. As the Blacklisted Crew says, HACK THE SYSTEM!

Ok, so we're getting back into reviewing hacking related items again. Several people have suggested ideas and submitted material for us to check out and to comment on, hoping to make the items known to the rest of the community. So, with no further adieu, here's our review content for this issue of Blacklisted! 411.

Cannon XL H1
Classification: Hardware (professional)
Cost: $9000 U.S.
URL: http://consumer.usa.canon.com/ir/controller?act=ModelDetailAct&fcategoryid=165&modelid=12152

Ok, so I recently got my mits on a pre-release of the Canon XL H1 3-CCD HD camcorder. I've been waiting patiently for this piece of gear to be announced by Canon. To my surprise, I had one show up at the office without any pre-notice from anyone. Needless to say, I was thrilled to be one of the first to handle one of these babies!! Anyhow, due for release in November or December 2005, this is no less than an INCREDIBLE unit. If you've been holding off on that Canon XL2 purchase, waiting for one of these, keep waiting. You'll be just as thrilled as I am. We own several of the Cannon XL2 camcorders already, so we're quite informed when it comes to using Canon gear. The XL2's, while they're great cameras, they've always lacked several options that, in my opinion, made them weak comparisons to other manufacturers cameras. Luckily, those options weren't deal breakers for us, so we were able to stick with Canon.

Upon first glance, the XL H1 is an impressive piece of equipment, no matter how you look at it. With an estimated price tag of $9000, let me tell you, you'll be getting more than you're paying for. The first thing I noticed when we pulled this out of it's box, it looks very similar to the XL2, but in black. Gives it a nice hi-tech look, too. It also feels like a professional piece of equipment. Have you ever picked up Sony's version of the HD camcorder? It feels like a cheap piece of plastic. Not the Canon. Boy, oh boy.

Digging into the actual use of the camera, how does it perform? Well, upon our initial testing, it's quite impressive. What did you expect? HD recording is done in 1080i. It will record in 60i, 30F and 24F. I'm thrilled that it has 24F as part of the lineup because it produces a very very good film-like picture. It comes with the built in ability to record still images at 1920x1880 which is NICE, plus the shoulder pad sports a professional "jack plate" (TC-IN, TC-OUT, GENLOCK, HD/SD SDI OUT) which means BNC connections, baby! The #1 problem I had with the XL2 was the lack of pro hookups and the lack of timecode in/out. Canon, this alone gets you two thumbs WAY UP! You've produced a fricken incredible piece of equipment.

Smugmug
Classification: Website (Image hosting service)
Cost: Starting at $29.95/Year
URL: http://www.smugmug.com

I happened upon this site while looking for an image hosting service so I could share family pictures with my extended family and friends in a secure fashion. Of course, I was going to do it myself, but then I started to think about my family... they're nt very computer literate and I had to come up with a solution for THEM more than for myself. I have to say that I looked at a lot of different image hosting sites, but none of them rung my bell. In fact, I was very unimpressed with what I had found... everything sucked or was geared toward selling on ebay. Not at all what I was looking for. Anyhow, I finally checked out smugsmug. Didn't think much of the name, thought it sounded lame like the rest of the sites I had visited. I was prepared to be completely unimpressed as I had been over and over again during this search. Anyhow, to say the least, I am fairly impressed with this site. So impressed, in fact, that I had to write a review on their site so I could get the word out. So, it's official, there really *is* an image hosting site out there that is all that you would want and more! Doing my research for the perfect place to share my photo's, I have come to the conclusion that whoever started up smugmug was tired of all the image hosting services out there being too costly for the little that you get. I'm willing to bet that they created their service out of their own necessity. I believe this because this is the only site that I could find that offered everything that I would want. And as many of you know, when you are using a service that is not up to your standards, you can't help but think of all the ways you could make it better. Well these guys went the extra step and did make their site better than the rest. They will not sell your email address so no spam, no annoying ads to look at, and best of all it's secure. You can make your photo's visable to everyone or make them only seen with a password. Your friends and family don't have to give up their email address or sign up in order to access your photos. One of my favorite features is the fact that anyone you give access to your pictures can have the option of downloading the pics to their own computer. On the flip side you can also protect your pictures from being downloaded. Now you're probably wondering how many pictures you will be allowed to upload. That's yet another beautiful feature of Smugmug! Unlimited pictures of any size! That's awesome! Ok, so I only touched on my favorite things, but there are so many different aspects to this place that I love. Please check it out for yourself. If you are looking for a place to store you pictures, then this is the place! I highly recommend them with two thumbs up! Oh, and did I mention that they are hacker friendly? Check it out for yourself under their hacking section.

I-Hacked
Classification: Website (hardware hacker)
Cost: $0
URL: http://www.i-hacked.com

I think this might be a first for me - writing a review of a website. I usually stick to hardware/software/videos, etc. Try to follow along with me. Anyhow, there's this hardware hacker website by the name of I-hacked (www.I-hacked.com) run by Heavnsnt. I've been on the site many times, looking around at their constant flow of articles since I'm big into hardware hacking.. I really like what they're doing and I can't help but to notice the great material and the HIGH traffic the site gets. Not bad. Not bad at all. One of my favorite articles is "Dirty MIRT" (Mobile InfraRed Transmitter) - it's a how-to on constructing a device that will force a traffic signal to give you a green light, just like the fire trucks and ambulances get. Anyhow, as much as I like it, I would never recommend building one of these or using one. Why? It's a federal crime! There's an article on hacking coke machines, google hacking, firefox browser hacking, etc. Yeah, so there are tons of articles and they're updated very often. As I'm writing this review, a couple of new articles just popped up. Nice. You have to visit this site. It's worth your time.

Make Magazine
Classification: Magazine (mainstream)
Cost: $34.95/yr U.S. $39.95/yr CAN $49.95/yr FOREIGN
URL: http://www.makezine.com

Published and backed by O'Reilly Media, Inc, Make Magazine is a very cool hardware hacker magazine. It's much more than a magazine, though. It's so fricken THICK and full of information, it's more like a book. In fact, they call it a "MOOK" which I thought was somewhat amusing. Produced quarterly, the cost of this magazine rings in at around $10 a copy. The magazine is a lot like the old electronics magazines (with all the DIY projects) mixed with a little hacking. It's a true hardware hacking magazine. It's very mainstream, too which is good for everyone. The have an opportunity to shine a good light on the hacker community. If you like WIRED, this one is SO much better. I had my first three issues sitting on my desk for almost two months before I finally had the chance to crack them open and soak it in. I have to say that I'm very impressed with the quality and the amount of information. It really blew me away. I'm so incredibly happy to see something like this finally being produced because it's backed so well, it will probably stay around for the long-haul. As a hacker, I feel that the more information sources available, the better off we all are. Keep in mind that because this is a mainstream product, you might get a little of that mainstream feel to it. (ie: shoving ads down your throat) Personally, I totally dig this magazine. I still think it's worth the money and definitely worth a look. To date, I've received four issues (every issue they've produced to date) and have been delighted with each issue. If you have not checked them out, please do so right away. I think you'll be pleasantly surprised by this find.

HUMANOID COMPANIONS

By The Goldfinger

If you think back to all the sci-fi movies and TV shows you almost always see robots or humanoid bots running around and interacting with humans. Star Wars had droids like C3PO and R2D2 and a host of other robots for various applications. Star Trek had Data, a humanoid android. The movie I-robot with Will Smith was another great example of humanoid companions. They were extremely "real" looking and capable of interaction. Check out their cool site too. During my research for this article, I came across another article in an unrelated genre that actually believed the site was real! Obviously they never seen the movie, or they would have known the NS-5 isn't quite possible yet. The site makes use of flash and I could see it fooling someone. (I didn't say who)

The fact that humanoid robots are always present indicates that they have become an accepted presence in society. The introduction of humanoid robots will impact our lives probably more than any other previous invention, including the car, the personal computer, and even the internet. They'll change society, our relationships and even redefine the family. It seems far off, but its coming.

As far as robots go, the first applications are likely to be from the military. In the United States, the overwhelming majority of financial support for robotics R & D comes from the Department of Defense. This isn't really a surprise since were always looking for bigger and better ways to kill people and blow stuff up.

Robots have been used in industry for some time, just look at the auto industry. Eventually, when consumer models crop up, we'll probably see a variety of task oriented models that will help us with household chores, light conversation and of course, recreation. This is where it will get very interesting. Sex robots will probably be in high demand. If they look real, and "feel" real, then you know they are gonna be a hit. More on that later…

For starters, imagine a domestic robot, acting as your butler or "household manager", that could communicate and control all the other robotic appliances and equipment in your home as well as do tasks such as taking out the garbage, retrieving your jacket from the upstairs bedroom, cooking dinner, and caring for your elderly live-in parent, how much time would that save you in a week?

The technology already exists and it can be done. In Japan, numerous high tech companies are developing companion robots and robots for many applications. A household robot would probably help reduce stress, and increase the quality of life. Once they work out the bugs, they can only improve. Humanoid development is in its infancy, and thats what we are witnessing now. The majority of humanoid development is occurring in Japan where half of its registered engineers are centered on robot intelligence and related fields.

Robots and Ethics

"The next great consumer technology will arrive in the form of personal robots". says Ron Arkin a Regents professor in the College of Computing and director of the Mobile Robot Lab.

"The innovations will be accompanied by a host of ethical concerns about human-robot interaction." adds Arkin, who co-teaches a course on robots and society with Charles Isbell, an assistant professor in the College of Computing.

"The introduction of robots to the general public may be sluggish at first, but it is inevitable." says Arkin, reflecting a consensus among roboticists worldwide. Among the tasks frequently mentioned as suitable for personal or domestic robots are housecleaning, cooking, helping care for elderly or disabled people, tutoring and secretarial tasks.

As robots become more animated and sophisticated, Arkin says, they may even be designed as humanoid companions, teaching humans how to dance, for example. Dance? No word on whether he meant vertically or horizontally although I will be covering robot intimacy more closely later.

Much of his lab's work aims to identify and combine the elements of reflexive behaviors with cognitive functioning to create autonomous, decision-making robots. The process is aided by techniques that help a robot "learn" from its interaction with the environment.

Human-robot interaction, military applications are some of the issues addressed in Arkin's robots and society class.

"What are we doing in terms of military applications? Is this appropriate use? Should robots be able to employ lethal force?" Arkin asks rhetorically. "At some point, do we trust the machines more than we trust ourselves? The Terminator movies seem to suggest we cannot trust the machines. I'm talking worse case scenario of course.

"My concern right now is not to formulate doctrine, but rather to formulate a consciousness among roboticists and robotic scientists that these questions need to be asked," he says. "Georgia Tech, through this course development, has provided me a wonderful forum to share those questions with my undergraduates."

Lots of really smart guys seem to agree that a few decades from now, give or take a few years, a C3PO lookin' droid is gonna be playing cards with your grandma, watching your kids, or delivering mail in your office.

"I have felt for years that the first 'killer application' of personal robots will be companionship, especially for the elderly," said Roger Brockett, a professor of computer science and engineering at Harvard University in Cambridge, Massachusetts. "Robots are potentially much smarter than dogs and they will not require the same level of upkeep."

Brockett, who founded the Harvard Robotics Laboratory in 1983, is one of several scientists who believe robots will some day be a part of everyday life.

Joel Burdick, a mechanical engineer and director of the Robotics Group at the California Institute of Technology in Pasadena, envisions personal robots as something akin to a very sophisticated handheld computer.

"They may remind people of their schedules as they leave the house, keep an eye on children while dinner is prepared, deliver mail in an office, dispense drugs at a hospital, all kinds of tasks that free up people, trying to make people's lives easier," he said.

Manuela Veloso, a computer scientist at Carnegie Mellon University in Pittsburgh, Pennsylvania, looks forward to a future where robots are as much accepted into daily life as the family dog or a newborn child.

"I'm interested in something that just co-exists with us rather than filling any holes, in the same way that when a human is born we do not need it, but it becomes a part of our lives," she said.

State of Robotics
Although a robot the likes of C-3PO is still a futuristic fantasy, the concept of human-like robots is currently very popular in Japan, said Burdick. "Japanese society is becoming very elderly and they think they will need more robots in the home to help out elderly people."

Honda Motor Co. of Japan is currently promoting what it calls the most advanced humanoid. Named ASIMO (Advanced Step in Innovative Mobility), the robot can interpret the postures and gestures of humans and move independently in response.

The company says in a statement that ASIMO can "greet approaching people, follow them, move in the direction they indicate, and even recognize their faces and address them by name." The robot can also access information via the Internet and use it to answer people's questions (in Japanese) about the news and weather. The last press release indicated there have been new developments in the ASIMO robot, and it is capable of running now! Check out their website and watch a clip of that lil sucker go!

http://world.honda.com/ASIMO/
http://www.honda.co.jp/ASIMO/

There are robots on the consumer market such as the Roomba Intelligent FloorVac from iRobot, which can vacuum your crib without you lifting a finger. The robot is a commercial venture of computer scientists and engineers affiliated with the Massachusetts Institute of Technology's Artificial Intelligence Lab in Cambridge.

Robot Sexuality
With all this innovation and research & development, I think it's a safe bet that, at least eventually, humanoid companions will become as common as cars and computers.

As robots get more sophisticated and more "real" looking, its inevitable that human nature will prevail and attempt to create Sex robots. Sex-bots, or whatever you want to call them will likely become a separate, if not popular industry within the humanoid companion genre. Enter the Masturbatrix.....

Almost every single sci-fi movie we've seen has alluded to, in one way or another, virtual or robotic sex.

Not necessarily displaying or advocating it, but alluding to it...they just never got into detail with sexuality in movies an shows like Star Wars, Star Trek, or Irobot.

Sex dolls are nothing new. What is relatively new are the innovations in them. Ultimately, the people that build and design these dolls are doing so with the concept of them being fully functional and interactive at some point, thus, a humanoid companion. A perfect example of very realistic looking sex dolls are the **RealDoll**. These hit the scene years ago and even Howard Stern "tried one out". He gave it a double fisted, enthusiastic two thumbs up. He said, and

I quote, "Best sex I ever had! I swear to God! This RealDoll feels better than a real woman! She's fantastic! I love her! This RealDoll is for real, I swear! Better than a woman! My wife isn't as good as that! May God take away all my ratings if I'm lying! I'll take a lie detector test! I swear on the life of my children! I did it and it was fulfilling! I did it and I'm proud of it! It was great! It was the best sex I ever had! Thank you RealDoll.com! It was fabulous! I could fall in love with that thing!" **Howard Stern**

After checking out their site, its amazing how real they look. And at a whopping base price of $6,499.00 they're not playing around. They have a few competitors as well. http://www.superbabe2000.com/frame1.html These don't look quite as good, but they are less expensive. A recent headline, taken from **Anano**va, read....

Robot Sex Dolls
A German inventor claims to have created the world's most sophisticated robot sex doll.

The sex androids developed by aircraft mechanic Michael Harriman from Nuremberg have 'hearts' that beat harder during sex.

They also breathe harder and have internal heaters to raise the body temperature - but their feet stay cold "just like in real life", according to Harriman.

He said: "They are almost impossible to distinguish from the real thing, but I am still developing improvements and I will only be happy when what I have is better than the real thing."

The dolls sold under the Andy brand name are on offer for ££4,000 each for the basic model, with extra charges for adaptations like extra large breasts.

Underneath the silicon skin, developed for use in medical surgery, is an electronic heart that beats faster during sex.

The model can also be made to move by remote control, wiggling her hips under the bedclothes and making other suggestive movements - all at the touch of a button.

Harriman said his design was an improvement on the popular 'real dolls' sold in the USA.
.....
The promise of high tech sex has come in various forms.

In Star Trek, they have the holo-deck, but they never really show you what its really capable of, or how far you can go with it. These are questions that not only space nerds want answered, but just about everyone would want to know if they thought these things were actually available.

Wanting to know myself, purely for academic purposes (cough), I discovered a few "devices" in the area of Teledildonics. Lol. Yes, I know. I get a kick out of that every time I hear it.

Teledildonics: dictionary.com definition is-
Sex in a computer simulated virtual reality especially computer-mediated sexual interaction between the VR presences of two humans.

This practice is not yet possible except in the rather limited form of erotic conversation on MUDS (multi user dimensions) and the like. The term, however, is widely recognised in the VR community as a 'ha ha only serious"projection of things to come. "When we can sustain a multi-sensory surround good enough for teledildonics, *then* we'll know we're getting somewhere."

Meanwhile, the best they have been able to come up with (to my knowledge) is the 'Virtual Sex Machine'. This system is, for lack of a better word, uh....um, lets do this..here are some excerpts taken from their site.

The **Virtual Sex Machine** consists of a small black box, some connectors and a device which looks like a penis pump. It hooks up to any standard 25 pin parallel (printer) port on your PC.

The available library of cd's contain sexually explicit material (porno!) or you can download special files. The machine comes with all the necessary cables and power supplies to install and operate your machine. No other equipment should be necessary.

And its made in America! MAC users, your outta luck! Not compatible. doh!
How do you operate it?

(excerpt)
This seems to be confusing to some people. We did not include manual controls for the device for one very specific reason. The purpose of the machine is to re-create a sexual experience. The concept behind the Virtual Sex Machine is

that you the viewer get to experience the action on the screen, as it happens, how it happens. It is portrayed as an actual sexual experience. Part of the attraction for the experience is the fact that you *don't know* what is going to happen next. You are also given pleasure without effort. You are not really in control of the situation, but are experiencing the fun without the effort. We are working on a version of the software that has override controls tucked away for those that need to have control over the experience. Stay tuned to our site for updates on this.

I can try to explain it to you all day, your best bet is to just check out the site and see for yourself.

http://www.vrinnovations.com/

They seemed to have gotten a lot of publicity from 1999 to 2003, and most of the feedback I saw was mixed. Seems like they got everyone really *aroused*, but then sort of didn't *seal the deal* or just *failed to deliver*. I've never tried it, so I can't give you a personal recommendation, but if anyone out there has one, or has tried it, email me an let me know.

After all is said and done, the promise of VR sex just isn't up to speed yet. And we still can't come home to our own personal humanoid companion that looks like Jenna Jameson, but until we can, brave men and uh, *mostly* men, will continue their quest to bring us closer to humanoid companions for all their many uses, and we salute them! Pz
the Goldfinger goldfinger@blacklisted411.net

Auditor: Debian WiFi Hacking

An article for those interested in wireless networking, but new to Linux.

By M L Shannon

Disclaimer

This article is for information purposes only; to learn about wireless hacking and security. Be aware that while intercepting signals *only* such as in Wardriving, is apparently legal, extracting text, graphics, and passwords is not. Also, it is unlawful to use someone else's AP for Internet access without their permission.

Intro

Wireless computing is the "in" thing. Businesses large and small are moving to wireless because it is easier and cheaper to set up. It eliminates the need for CAT-5 cables and the expense of stringing them through the facility. The same applies to home networks, thanks to WiFi one can inexpensively install a DSL router and Access Point and take a portable out in the back yard or wherever, and connect. Wireless cafe's are opening by the hundreds for people who find them conveniently near their job, or a place to relax and get cheap or free broadband access.

Many such businesses are unaware that their connection to the Internet is far from secure, as are most individuals. The results of many wardriving exercises reveal that well under half of the APs detected use WEP encryption, which, at best is to most people is a false sense of security. WEP can be defeated.

I learned from my years in surveillance and countermeasures, that the only way to be secure from electronic eavesdropping is to know how it works. The same is true of wireless networking.

This, the first in what may be a series of articles, is about maintenance, testing and hacking using the Debian Linux Auditor suite of applications.

For this first article we will go over only a few, the most important applications, which are those that

1. Detect WiFi APs and Ad Hoc mode cards
2. Intercept text packets
3. Spoof, or change the MAC of a wireless card.

Auditor is a powerful and sophisticated suite of programs, applications that you download as a single file and burn to CD as an image. You can run Auditor from the bootable Linux CD, or you can install it on your HD as dual boot and still have your existing OS, whether Windows or BSD.

Why Auditor compared to Win Apps?

First of all, Auditor is free (although donations are accepted) and then there aren't, that I know of, any complete Windows 'suites' like Auditor. Auditor also contains text and hex editors, screen capture, graphics programs, Firefox for WWW and lots more. All on a single disk.

So, you can run the Auditor suite with your present OS intact, remove the CD and reboot and your computer is just as it was before you ran Auditor.

And also, not everyone can justify the expense of a dedicated portable just for Auditor

There are indeed some excellent wireless applications for Windows, and two that, far as I have been able to find, have no Linux counterparts.

The first of these is CommView for WiFi. This is a great program, with which you can search for APs, and once found, view both text and graphics. (Is that your neighbor across the street, the sweet little blue haired lady, downloading hard core porn?) CommView is versatile and powerful and has the most comprehensive set of filters (Called 'rules') I know of. You can filter packets in (see on screen) or out (block) by MAC, SSID, text string, port, data, control and management packets.

I had the pleasure of meeting the author while I was in New Zealand.

The second is Iris, with which you can see what is on the monitor of the AP you are monitoring in real time. I have played with the demo, and it appears to be one helluva program. It goes for about US$1200.00.

So, for real time viewing of the target, these two Win apps might be the better choice, but for serious detection and analysis, and hacking, Auditor is the answer.

System Requirements

While I don't see this listed on the Auditor site, I would suggest at least:

Pent II notebook; laptop, at 500 MHz or faster
128 MB RAM.
CD burner, such as Nero.

Wireless card that can run in Radio Monitor Mode and an antenna. Before you buy, be aware that most PCMCIA cards do not have a connection, jack, for an external antenna, so it is a good idea to check before you buy. Determine what kind of jack, MMCX for example, and then obtain an antenna with the right cable.

Auditor will, of course, run on a desktop but some of the applications in Auditor may not like PCI cards or WiFi cards on an ISA Adapter, and anyway, once running you will likely want to do some field testing. A shopping cart with a couple car batteries provides plenty of space, and it is easy enough to mount a hi-gain antenna but this is rather conspicuous; it may well draw unwanted attention.

Many WiFi cards are supported and driver installation is not required as Auditor loads them automatically.

I have tried Auditor with a Linksys WPC-55AG dual band and Senao NL 2511 CD Plus Ext 2, and both work automatically. The old classic Orinoco Gold also works but the newer Proxim 8420 WD does not. For that matter, the Proxim doesn't work on much of anything Windows so is not recommended. Perhaps later Proxim models work, see the Auditor FAQ at

http://new.remote-exploit.org/index.php/FAQ_main

The Senao has external antenna connections (2) as does Proxim, some SMC cards, and the classic Orinoco Gold, but again, most do not.

So without an antenna, unless you are within a short distance of an AP, from a few dozen meters to maybe across the street, you may not see much signal strength. But radio waves work in mysterious ways, so you never know.

Radio Monitor Mode

In this mode, also known as raw monitoring mode, the WiFi card will receive only; it will not transmit. It is strongly recommended that it be used to prevent anyone from being able to detect you while you are detecting them, and prevents accidentally associating with (connecting to) an AP you are monitoring. Instructions on how this is done is at http://new.remote-exploit.org/index.php/FAQ_main.

To find out what chipset a given card uses, go here:
http://www.linux-wlan.org/docs/wlan_adapters.html.gz

Back up everything!

Even though you are not likely to damage any files using Auditor, it is still a good idea to make backups of all important files. Just in case.

Downloading and Installing

Auditor, which is more than 600 Mb in size, is downloaded as an ISO file from any of several sources, listed here:
http://new.remote-exploit.org/index.php/Auditor_main
http://new.remote-exploit.org/index.php/Auditor_mirrors

It takes a couple hours depending on your download speed. If you are using dial-up, or for whatever reason don't want to download something that large, you can send email mmo@remote-exploit.org to see if someone will snail mail you a copy of the latest version.

If it downloads successfully, you can go ahead and burn it, but then you have the option of checking MP5 which is a hash algorithm to verify integrity of the file. I skipped this and just fired it up, and... it wouldn't run. Oh, it tried, I got the boot screen, but then a long series of error messages, including media error, buffer I/O error and on and on.

Being a newbie to Linux, I had to look up them but the explanations still didn't tell me what was wrong.

Finally it dawned on me that I read somewhere on the Auditor site that I should burn the CD at a slow speed, 8x or even 4x.

I did this and Auditor was up and running.

Burning

Once you have downloaded the file, you need to burn it to a CD as an image file. This is not the same as an ordinary data file. If necessary, read the help files for the program you are using.

With Nero, you want *Disk Image or Saved Project.* Other applications, look for *burn as an image.*

Now this may be important: If you burn the CD at the fastest speed your drive is capable of, the CD might not work. I found this out the hard way by not reading the help files. Burn it at 8x or even 4x.

Starting Auditor

First, you may need to change your BIOS settings so the machine will boot from CD.

Once the ISO has been burned as an image, pop the disk into the drive and reboot.

Problems Running Auditor

Even if the disk boots, it might not install in RAM. It may appear to be trying but will display a long list of errors such as Fatal Exception in Interrupt, Segmentation Fault, Not Synching, Unable to Mount Root and ending in the fatal Kernel Panic.

Also, the CD may run a few times and then just quit completely. This happened the first time I tried Auditor, and even after learning about the slow burn, the same thing happened.

I suspected it was because of this crappy computer, a Compaq Presario 2700, (You don't want one) but I heard the same story from a few others.

Install Auditor on the hard drive

Auditor has this option, to HD install. Open the KDE menu, and under All Applications, System, at the top is Auditor HD Installer.

There is an advantage of doing this: If you have a computer that does not have both the CD and floppy drives, there is nowhere to save the files you build from scanning (Auditor is running a RAM disk) unless you install an external hard drive. Fine for at home, but inconvenient for field works as they require external power. Now if the drive is not partitioned for dual boot, you are running

Windows and want to keep it, the alternative is:

Dual Boot

Some people can dual boot with no problems at all. Someone at a recent 2600 meeting had a machine that was triple boot; Win 2000, Red Hat and Free BSD as I recall! Others find it difficult, especially those new to Linux. My first attempt was somewhat tricky but fortunately I bought the Red Hat Pro box version and by reading the manuals I got through it OK.

But: there is a better way:

Partition Magic.

I bought PM years ago for whatever reason, but had never used it; didn't trust it. Didn't want to take a chance on losing or screwing up files. But I have since purchased a Western Digital external 80 Gb drive (I can't say enough good things about WD; have bought their drives since Connor merged with Seagate or whatever it was that they did) and have never had a problem. So I backed up everything on the Compaq and fired it up.

With PM installation was flawless, I followed the default settings and only a few times did I have to look up anything. As with any flavor of Linux, you will need to set a root account and one or more user accounts.

NOTE: While it may be possible to change settings to prevent this, some of the wireless apps run only from root. Fine as long as you don't fire up Xchat and get kicked off an IRC server for logging on as root :)

It took about an hour on the Compaq 30 Gb drive, and when I rebooted, up came Grub and the dual boot option screen. Auditor is the default and comes up automatically unless you choose Windows.

The opening screen takes a couple minutes to load, then there is a toolbar at the bottom of the screen with several icons. The installation includes text editors, Firefox for WWW and many other applications.

Using Kismet

The first of the applications in this article is Kismet, of which there are two versions. The first is the original Kismet, the other is Gkismet, a GUI for Kismet.

Open KDE. To get to the applications, scroll up to Auditor, then Wireless. Then Scanner/Analyzer. There are two selections. Kismet Tools and Wellenreiter. Kismet are the main tool with which to get started. Later, after you are intercepting Access Points, you can try Wellenreiter, spoof your MAC and see what's in the packets using Ethereal.

When you click on Kismet, you will be asked to choose a Data Directory. For now, you can use most anything, such as the tmp directory under your user name. Next click Yes to confirm the location, then OK on the next prompt; Desired Fileprefix.

Now, Kismet starts running. Click the up arrow to run full screen if desired.

Unless you are in an isolated area, there will be at least a few listings. On the left is the name of the network; the SSID or Station Set IDentifier. The rest of the columns contain details of the APs or AdHoc's you are receiving. Click 'h' for the Help screen which explains what most of it means.

Kismet starts in autofit sort mode, so you won't be able to expand the listings. To change it, you need to use command line from Konsole. More on this is in the help files and Forums listed at the end of this article under Getting Help.

Using Gkismet

Start it the same way, Auditor, Wireless, Scanner/Analyzer. When the screen loads, you should see the same listings as with Kismet but this version is a little easier to use. On the left are two icons.

The icon with a little triangle shaped flag, a pennant is an Access Point:

The icon is of a little computer is a Probe Request; A signal being sent out from a WiFi card, looking for an Access Point to connect to. (If in RMM no signal is sent; the card is silent and undetectable.) Also known as Ad-Hoc mode where one computer associates directly with another and not through an Access Point.

Click on the + for any listing and it expands to display detailed info on the signal. Most of it isn't important yet; this is about getting started, so can be disregarded for now. The main things are the SSID, signal strength, and WEP.
Click on View and you can sort by signal strength or munber of data (not control) packets.

Once you see packets being captured, you can open either Packet Dump or Screen Dump and see what is being intercepted.

Using Ethereal

OK you now are able to use Kismet and have presumably found a few APs or AdHoc cards, and you want to know what kind of information is being transmitted. The KDE menu path is Auditor/analyzer/Network/Ethereal.

Double click to start it, then on the top menu bar, select Capture, Interfaces. Pick one of the devices (You will see the difference when you have tried both) and click on Prepare.

If you want Ethereal to display the packets it logs in real time (Rather than storing in a file)

Update list of packets in real time and then capture.

A window will open on the right showing numbers of captured packets and you will see them on the main screen.
As long as you have found at least one signal in Kismet, you should see packets.

Hardware Suggestion

If you have more than one wireless card, consider getting a pigtail for each. This eliminates the need to disconnect the cable when you switch cards. The plugs and jacks, while manufactured to close tolerances, are so small that frequent plugging and unplugging can eventually make them loose and requiring replacement.

Troubleshooting

Auditor is up and running and I have started Kismet, but I don't see anything on the screen.

Either you are in an ice cave in Antarctica or a rural area without an external antenna. Try visiting a wireless cafe'.

I see lots of signals, they are all Access Points, but when I run Ethereal, all I see are like garbage packets, meaningless digits and characters.

What you are seeing are management and control packets, and no one is using the AP at the time, or packets from a WEP encrypted Access Point.

Understanding signal strength

The strength of a WiFi signal you intercept may be measured in different ways with different applications. Technically, it is measured in decibels, dB, but different applications use different methods. So, what numbers you see with one program don't necessarily relate to another. What counts is if the signal is strong enough that you can intercept and read the packets. So, it is not necessary to spend time learning this.

Where to Get Help

http://new.remote-exploit.org/index.php/FAQ_main
http://new.remote-exploit.org/index.php/Tutorials

Sources, PC Cards

Most computer stores sell wireless cards. Very few of them sell cards that have an external antenna connection. And if you search most online sources and read the specs on the cards that they do have, you aren't likely to see if they do have an antenna connection.

Seattle Wireless, http://www.seattlewireless.net/ has lots of good information.

Two of the best cards are the Senao and the SMC 2835W. Both are compatible with Linux and Unix; Free BSD for example.

Finding the SMC (with the antenna connection) is problematic; you'll find it where you find it or order online

Surf & Sip sells the Senao, with two antenna jacks, for about $90.
http://www.surfandsip.com/location.htm

The old Orinoco Gold card is good for monitoring, but has less sensitivity than the SMC or Senao, both of which have a much higher power output when used for your own network. Or whatever else.

The Proxim 8420-WD, which does have an antenna connection, does not work with Auditor, or hardly anything else.

Sources, Antenna Cables

This can be difficult, as there are many types of connectors, so again, find out what you need for connecting an external antenna when you obtain the card. Probably the best source for pigtails and extension cables is www.therfc.com in Maryland. They have been in business for many years and their products are excellent. They are the only place I will buy from.

BLACKLISTED! 411 MAGAZINE

PRESENTS

HACK THE SYSTEM!

(the DVD)

Our latest project is in the works, and will be coming soon to a DVD store near you!

We're putting together a brand new DVD about hackers, the hacker community, technology and all related issues. The DVD is arranged as a documentary with a mix of "reality TV" thrown in to capture the interest of a wide audience - old school & newbie hackers, teens, college students and professionals alike. Packed with interviews from the Blacklisted! 411 staff, contributors, real life hackers (both white hat and black hat), celebrities, industry leaders, law enforcement and local government, this won't be your average hacker video. It's the ideal of the Blacklisted! 411 team to bring to the table an informed look at hacking, the reality, the pitfalls and associated amusement. We're serious, but we'd like to keep it fun, too.

You asked for it, so here it is!

Meet many of the Blacklisted!411 staff

Meet our own Editor in chief, Zachary Blackstone! You'll also finally be able to meet the infamous, octopus wearing, Extreme Kidnapping's very own Goldfinger! You'll also meet Ghetto Mafia of our "street crew" and many other staff and crew members!

Live tutorials and how-to's

See how a red box is really made and what it does. Watch wardriving in action. Caller ID spoofing, social engineering, and how to find goodies at a salvage yard. Just a few of the "must see" things which will be available on this DVD.

Fascinating interviews of law enforcement officials, hackers in the news, and software moguls

You'll enjoy what other members of the hacker community have to say. Some from behind bars, some previously behind bars, some rich dudes that got their start from hacking, and some hackers we met on the street. Not to mention you'll love to hear what law enforcement officials really thinks about hackers.

Hilarious comedic skits

Who wants to watch a DVD with boring all talk, talk, talking? You'll see skits that rival any of the popular reality jackass skits out there! Hear some hysterical phone pranks, and many more skits and pranks that will leave you either speechless or rolling on the floor laughing!

Clips of the most outrageous "for hackers only" beach party

See the ad in this issue for more info on the Blacklisted! 411 end of summer beach party. Be sure to be there, you might see yourself on the DVD!

If you'd like to learn more about the DVD, or if you would like to contribute to it, please check out the website at:

WWW.HACKTHESYSTEMDVD.COM

Internet Insecurity

By Dr. Fibes

If you've been reading the mainstream tech news you may have noticed that cracker attacks and the like have been increasing dramatically as of the last year or so. It appears that many of those that once took delight in learning the vulnerabilities of the net just for the sake of knowledge have now crossed over to "the Dark Side", using their abilities for less noble purposes, such as gleaning money. Your money.

If you're like many of us, you may have a false sense of security. After all, in spite of the dire warnings we've all read about for years, many of us haven't really experienced any problems of note.

That doesn't mean that these security risks are not that big of a deal. It just means we've all been lucky.

As these "black hats" become more proficient, the danger ramps up to each and every one of us. It's currently increasing at a rate such as we have not experienced before.

It's not all gloom and doom though. We have options that are new and very difficult to circumvent. That will be the primary focus of this article. There is much information about this subject on the web. It is my goal to present this information to you here in one place, to save you many nights of reading arcane pages that will put you to sleep.

Probably the most basic and easily used tool in regards to the security of your machine is a firewall. Almost everyone is somewhat familiar with firewalls. These are available in both software and hardware varieties.

From the viewpoint of security, the hardware firewall probably has a slight edge. It's easy to comprehend that a malicious TCP packet from evilone.com can do you absolutely no harm if it doesn't even make it to your machine. It's like the bouncer at your party, no undesirables can even get past the front door. Assuming of course, that it's properly configured and well designed.

But practically speaking from a home consumer point of view, a software firewall will work just about as well. A dedicated hardware firewall starts at about $350 and the sky's the limit. There are decent software firewalls available for free. The Windows XP SP2 firewall is pretty good, except that it only works on incoming packets. This means if you were to get something like a Trojan in your email, it could compromise you by relaying sensitive information outgoing to who knows where. It's unlikely that you would ever know.

Although I have not personally used it, ZoneAlarm gets pretty high marks from the security gurus on the net. And the personal home version is free. There are at least 2 or 3 other free firewalls that are commonly recommended. Not all are created equal, so I recommend you continue reading this article, I will be discussing what you want to look for in a firewall.

Getting back to software firewalls, another advantage is that they can be updated at any time. So as new methods of exploitation become known, the software author can implement countermeasures and make them available for download in a timely manner. This can be more difficult or even impossible with hardware firewalls.

The biggest downside to software firewalls is that they utilize your system resources, and that means stealing some of your machines time, which really means YOUR time. Hardware firewalls operate independently, so this is not an issue.

Most routers also come with a hardware firewall. These can be the best solution of all for the home user. The newer ones are often very comprehensive and inexpensive. I personally prefer this method for my home use, primarily because most of them contain at least a NAT firewall. And another layer of firewall as well.

Routers that have a NAT (Network Address Translation) firewall are very desirable because they essentially hide your machine(s) from external sources. The only externally visible information available from you is the IP address of the router itself. This is NOT your machine's IP address. It is impossible for anyone to see your IP through a NAT firewall. The router assigns these to your machines, usually something like 192.168.0.100 through 192.168.0.199, each new machine gets the next number in line. An address of this value is never assigned to a machine coupled directly to the net. You could have 25 machines on that router, all they can see is the one IP address of the router. However, you should be aware that Java is happy to give out your private IP address and the only way to stop it is to disable scripting. The NAT firewall can prevent your IP address from being seen externally, but it can't keep you from freely giving it away.

You should also be aware that by the use of a technique called fingerprinting, some information can still be leaked through. Carefully formed TCP packets can be sent that cause the operating system name and version of your machine(s) to be disclosed. It's very likely that in the future your greedy ISP will do exactly that to reveal how many machines are on the other side of the router. They like to limit the number to a few machines, so that they can artificially charge you for more machines, when their real concern should be your bandwidth usage. Sigh.

There are methods to spoof this information. You can find them by searching for "fingerprinting spoof". Knowing the operating system is very valuable to a bad guy trying to do you harm. He needs to know what operating system you're using in order to decide which method of attack to use. In a future article we'll explore those methods.

As stated previously, there is often another firewall layer on these routers. These primarily take the form of Packet Filtering or Stateful Packet Inspection. This same information applies to software firewalls.

If at all possible, you want to get a Stateful Packet Inspection firewall, also known as Dynamic Packet Filtering. Packet Filtering, also known as Static Packet Filtering simply examines a packet's header information.

The more robust Stateful Packet Inspection examines not only the header information, but also what's going on up through the application layer. It tracks each connection and all of its interfaces through the firewall, making sure that it is valid. In this manner, it can determine more than just source and destination information. It does this by monitoring the state of the connection and keeping track of it in a table. This allows it to filter packets not only according to the rules that you have defined, but also based upon prior packets that have passed through it. Additionally, RPC (such as Frontpage Server Extensions) and UDP (such as Domain Name Resolution from your DNS server) applications can work seamless with it, because it creates virtual session information for them. No other firewalls can do this.

Now most of these routers come with pretty wide open specs to limit the amount of customer support they have to provide. This is understandable; after all, why should they have to teach you all about firewalls? So in order to use them effectively, you must go to the router configuration screen, almost always a unique address in your browser that communicates directly with the router itself.

Some of the things you'll want to be sure to lock down:

(Note: Not all firewalls have all of the options listed here, you'll have to determine what's appropriate for yours)

Respond to the ICMP (ping), DON'T. Many crackers use software that is the modern-day equivalent of wardialers to seek out vunerable machines. They ping hundreds of thousands of addresses per hour looking for addresses that have a machine on them. Don't be seen.

Denial of Service firewall – DO. The reasons are obvious.

Remote Administration – DON'T. Do you really need to remotely access your firewall? This is almost never needed and provides a security hole. You can administer the router from any of the local computers.

Allow Trusted Stations Only, DO. Unless you intentionally have pedestrian computers (a friend's laptop for example) visiting your router limit access to only those computers that you know of. If you have the same friend over all the time with his laptop, you can just put him on the trusted list. MAC addresses can be spoofed, but this provides yet another layer of protection. And that's all you've got, layers.

Broadcast SSID, DON'T. Hey, you know what it is, don't you? Why tell the world. Give them yet one more hurdle to overcome.

Use WPA, DO. Don't use the WEP encryption, it's a joke. While WPA can be cracked too, it's tougher, requiring the acquisition of hundreds of thousands of packets. Layers. And while we're on the subject, use a keyphrase that is 20 characters or more in length and includes numbers and letters. The more random the better, "mary had a little lamb3" is not what we're looking for. Don't help them to crack your key.

Block access control for any port you're not using. Which ones are these? That depends on what software you use. One thing's for sure, it'll be almost all of them. Some of the most commonly used TCP ports are:

Port 80 for web browsing
Port 443 for secure web browsing
Port 21 for ftp
Port 25 and 110 for email
Port 119 for nntp (usenet)
Port 5190 for AIM
Port 53 and 113 for DNS service

Port 23 for Telnet
Port 1863 for MSN messenger
Port 5190 for ICQ

Not a comprehensive list by any means, but it'll give you an idea. Note also that non-standard ports can be used for any of these functions, for example, you may access an ftp server on many ports, not just port 21, depending on the server. So just do your best, and check your various programs to see if they still function correctly. If not, find out what ports they are using and open those.

Most good firewalls will also stealth the ports. This means that they won't respond if someone tries to send a request to them. Why is this important? Because even if a port is CLOSED, it will respond to a request packet and you can be compromised through it with a TCP stack exploit.

OK, so now you've set up your firewall, and everything appears to be working correctly. How do you know if you're secure?

First of all, you're not. You've just made it a lot tougher. But let's check and just see how secure you are.

There are many web-based firewall checks, some are better than others. One of my favorites is http://www.auditmypc.com . They often surprise me, just when I think I've got it all buttoned up. They have one page I find very informative also: http://www.auditmypc.com/security-patch.asp

Some of the things you find there may surprise you.

But there's many others, so just go to Google and look for "firewall test" to try others.

You do use Firefox, don't you? If not, I highly recommend it over the bloated insecure pig that Microsoft puts out. Hevnsnt has a great article on the blacklisted411.net website about using Firefox.

I also suggest downloading a copy of NMAP, you can get it from http://www.insecure.org/nmap. It's common for folks to use that wonderful program to look for ways to exploit you, why not beat them at their own game? Just look in your router administration screen for the IP address of the router (the true external IP), and run NMAP to check that IP, it's that easy. Be sure and spend a little time at insecure.org learning how to use NMAP, it has a lot of options.

After all is said and done, you still cannot be completely secure. So the best thing to do is to shut down your machine when you're not using it. There's plenty of folks out there that just leave their machine on 24/7, they're just asking for it. If your machine's not on it's not a security risk. The days of leaving personal computers on all the time are over. Back in the day it was said that it was "better for the computer" or "better for the hard drive" to just never shut it off. I really don't know if that was true or if we just convinced ourselves of it because we didn't want to wait for that startup on those slow 4 meg. machines. But now it's a moot point, because modern hard drives and motherboards definitely do better when allowed to cool down now and then. Just ask an old desert rat like me. It gets hot in the Mojave. If you leave it on all the time out here, you'll be buying a new machine quite often.

Think this is all a bunch of "the sky is falling" malarkey? Go on over to auditmypc and let them show you your internal IP address right through your shiny new firewall.

Still not convinced? Here's a copy of the access control log for my firewall this morning as I finished this article, about 2½ hours worth. I also had one attempted denial of service attack not shown.

Good Luck.

Date	Time	Name	Source IP Address	MAC address (HW address)	Destination	Port
2005-10-20	09:07:16	Unknown	207.68.178.16	Unknown	LAN(TCP,port 43273)	WAN
2005-10-20	09:07:16	Unknown	207.68.178.16	Unknown	LAN(TCP,port 42505)	WAN
2005-10-20	09:10:47	Unknown	66.167.248.178	Unknown	LAN(TCP,port 34560)	WAN
2005-10-20	09:12:23	Unknown	63.210.164.47	Unknown	LAN(TCP,port 43529)	WAN
2005-10-20	09:12:30	Unknown	72.244.123.146	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	09:12:32	Unknown	65.200.201.29	Unknown	LAN(TCP,port 44553)	WAN
2005-10-20	09:13:06	Unknown	63.210.164.41	Unknown	LAN(TCP,port 58889)	WAN
2005-10-20	09:13:06	Unknown	63.210.164.41	Unknown	LAN(TCP,port 58377)	WAN
2005-10-20	09:14:15	Unknown	66.218.70.162	Unknown	LAN(UDP,port 39689)	WAN
2005-10-20	09:16:34	Unknown	83.211.241.203	Unknown	LAN(TCP,port 61719)	WAN
2005-10-20	09:18:00	Unknown	80.189.165.189	Unknown	LAN(UDP,port 35072)	WAN
2005-10-20	09:27:56	Unknown	72.244.124.50	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	09:28:39	Unknown	65.91.108.146	Unknown	LAN(TCP,port 39173)	WAN
2005-10-20	09:28:54	Unknown	72.245.2.72	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	09:41:37	Unknown	66.167.231.170	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	09:49:57	Unknown	72.244.56.80	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	09:54:42	Unknown	72.43.77.210	Unknown	LAN(TCP,port 48385)	WAN

Date	Time	Name	Source IP Address	MAC address (HW address)	Destination	Port
2005-10-20	10:03:40	Unknown	69.3.58.202	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	10:06:33	Unknown	66.94.230.125	Unknown	LAN(UDP,port 57352)	WAN
2005-10-20	10:07:35	Unknown	72.244.67.112	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	10:09:55	Unknown	72.244.124.38	Unknown	LAN(TCP,port 35584)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 5120)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 5376)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 5888)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 5632)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 6400)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 7936)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 10496)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 12288)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 12800)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 20480)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 15104)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 20224)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 25344)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 20736)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 28160)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 30464)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 31488)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 34048)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 34816)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 34560)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 35584)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 35072)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 36352)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 37376)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 43520)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 19969)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 42241)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	10:11:45	Unknown	198.64.140.152	Unknown	LAN(TCP,port 41985)	WAN
2005-10-20	10:12:43	Unknown	207.68.178.16	Unknown	LAN(TCP,port 13577)	WAN
2005-10-20	10:12:43	Unknown	207.68.178.16	Unknown	LAN(TCP,port 13321)	WAN
2005-10-20	10:13:57	Unknown	66.102.7.99	Unknown	LAN(TCP,port 10250)	WAN
2005-10-20	10:14:00	Unknown	66.102.7.99	Unknown	LAN(TCP,port 266)	WAN
2005-10-20	10:14:43	Unknown	216.239.57.147	Unknown	LAN(TCP,port 18954)	WAN
2005-10-20	10:17:21	Unknown	198.65.111.254	Unknown	LAN(TCP,port 43530)	WAN
2005-10-20	10:17:40	Unknown	66.218.70.160	Unknown	LAN(UDP,port 59912)	WAN
2005-10-20	10:18:04	Unknown	198.65.111.254	Unknown	LAN(TCP,port 22538)	WAN
2005-10-20	10:18:55	Unknown	72.244.191.84	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	10:19:31	Unknown	63.210.164.23	Unknown	LAN(TCP,port 14089)	WAN
2005-10-20	10:19:31	Unknown	63.210.164.41	Unknown	LAN(TCP,port 12809)	WAN
2005-10-20	10:19:31	Unknown	63.210.164.41	Unknown	LAN(TCP,port 12553)	WAN
2005-10-20	10:19:33	Unknown	63.210.164.25	Unknown	LAN(TCP,port 15881)	WAN
2005-10-20	10:21:20	Unknown	72.244.118.246	Unknown	LAN(TCP,port 34560)	WAN
2005-10-20	10:28:04	Unknown	72.244.124.139	Unknown	LAN(TCP,port 34560)	WAN
2005-10-20	10:29:29	Unknown	216.239.57.147	Unknown	LAN(TCP,port 39695)	WAN
2005-10-20	10:33:07	Unknown	198.65.111.254	Unknown	LAN(TCP,port 52750)	WAN
2005-10-20	10:37:13	Unknown	207.68.178.16	Unknown	LAN(TCP,port 53265)	WAN
2005-10-20	10:40:36	Unknown	72.244.117.246	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	10:41:57	Unknown	201.133.162.228	Unknown	LAN(UDP,port 35072)	WAN
2005-10-20	10:44:37	Unknown	72.244.127.244	Unknown	LAN(TCP,port 34560)	WAN
2005-10-20	10:44:59	Unknown	207.46.250.119	Unknown	LAN(TCP,port 28936)	WAN
2005-10-20	10:48:05	Unknown	207.68.179.219	Unknown	LAN(TCP,port 40712)	WAN
2005-10-20	10:51:05	Unknown	207.68.178.61	Unknown	LAN(TCP,port 33032)	WAN
2005-10-20	10:52:43	Unknown	72.244.124.59	Unknown	LAN(TCP,port 34560)	WAN
2005-10-20	10:57:34	Unknown	72.244.124.220	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	10:59:38	Unknown	83.32.239.189	Unknown	LAN(UDP,port 35072)	WAN
2005-10-20	10:26:31	Unknown	202.99.172.160	Unknown	LAN(UDP,port 516)	WAN
2005-10-20	10:39:01	Unknown	72.244.114.135	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	10:39:34	Unknown	72.244.127.99	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	10:44:06	Unknown	72.244.67.125	Unknown	LAN(TCP,port 48385)	WAN
2005-10-20	10:45:09	Unknown	72.244.67.125	Unknown	LAN(TCP,port 35584)	WAN
2005-10-20	11:08:50	Unknown	66.102.7.104	Unknown	LAN(TCP,port 2564)	WAN
2005-10-20	11:09:03	Unknown	216.239.57.103	Unknown	LAN(TCP,port 14852)	WAN
2005-10-20	11:12:17	Unknown	198.65.111.254	Unknown	LAN(TCP,port 22788)	WAN
2005-10-20	11:17:23	Unknown	72.244.114.130	Unknown	LAN(TCP,port 35584)	WAN
2005-10-20	11:21:08	Unknown	72.244.127.34	Unknown	LAN(TCP,port 34560)	WAN
2005-10-20	11:22:34	Unknown	202.99.170.138	Unknown	LAN(UDP,port 39429)	WAN
2005-10-20	11:26:48	Unknown	216.239.57.99	Unknown	LAN(TCP,port 25867)	WAN
2005-10-20	11:29:33	Unknown	198.65.111.249	Unknown	LAN(TCP,port 26123)	WAN
2005-10-20	11:29:33	Unknown	198.65.111.249	Unknown	LAN(TCP,port 34059)	WAN
2005-10-20	11:30:00	Unknown	206.16.239.232	Unknown	LAN(TCP,port 64012)	WAN
2005-10-20	11:32:35	Unknown	216.239.57.96	Unknown	LAN(TCP,port 34573)	WAN

REMOTE ENCRYPTED DATA ACCESS

By dual_parallel

Do It Ourselves

You've seen them. Articles about "setting up such-and-such server on your home cable" and "getting this-and-that access using your home DSL." Those are fine for your power user who knows more than a Compoosa employee and less than a LUG attendee. This article takes the basic concept of the do-it-at-home article to the next level, for such an aware Community needs proportionate security and mobility.

Security and mobility are exactly what this project provides. For example, imagine yourself at the local cafe: good coffee, relaxing atmosphere and free Wi-Fi. It's the perfect spot to kick it and get some work done at the same time. You're banging away on your article and slap yourself in the forehead. You forgot your research data at home!

Oh wait. No worries. You can grab the files you need wherever there's net access. But every noob with Ethereal is going to get your passwords and data. No worries again. You have easy-to-use encrypted access to hundreds of gigs of file storage. Ah. Good mocha.

Prerequisites

To executively summarize, we'll build an NFS server, build an SSH server, mount the exported file space, and setup gFTP for file access. It is assumed that the reader has broadband access and a hardware firewall, or router. Note that home broadband upload speed is the bottleneck in this system. Red Hat Enterprise Linux (RHEL) and nano are used throughout.

The reader is responsible for keeping an up-to-date box. Enterprise Linux uses up2date, and apt-get is another of many options. The reader is also responsible for creating backups if a configuration goes south.

```
# cp config.file config.file.bak
```

Build the NFS Server

Network File System (NFS), created by Sun Microsystems, allows network shares to be used as if they were local. NFSv3 is insecure exposed to the Internet, hence this configuration. We'll export drive space from a dedicated file server to the SSH login server, which faces the Internet. On to the build.

Be resourceful and find an older computer and a large hard drive. Combine the two. Partition the drive to include a separate partition to export - that is, to share across your network. Here is an example partitioning scheme for a 120GB hard drive:

/dev/hda1	/boot	100 MB
/dev/hda2	/	13000 MB
/dev/hda3	swap	768 MB (2x 384 MB RAM)
/dev/hda4	EXTENDED PARTITION	
/dev/hda5	/export	100000 MB

This scheme gives an /export partition of 100 GB, which is more than enough of space for this application. Now install GNU/Linux with the minimum of components. X is optional. NFS and RPC are necessary, which RHEL installs by default. Users won't be needed on this system, as it's solely a file server and only root is necessary for administration. Enable portmap and nfsd for your run level using system-config-services. Also, shutdown any and all unneeded services, i.e. pcmcia, sendmail, etc.

Create a data directory in the /export partition, make it world-writeable, and set the sticky bit.

```
# mkdir /export/data
# chmod 1777 /export/data
```

Edit /etc/exports and add the following line, entering the appropriate host name or IP address.

```
/export/data SSH_HOST (rw,async)
```

Restart portmap and nfsd.

```
# service portmap restart
# service nfs restart
```

Set up tcpwrappers - /etc/hosts.deny and /etc/hosts.allow - to only allow NFS connections from the login host.

```
# nano /etc/hosts.deny
ALL : ALL
```

This denies all access from all hosts. Now poke holes with hosts.allow.

```
# nano /etc/hosts.allow
portmap     : SSH_HOST : ALLOW
lockd       : SSH_HOST : ALLOW
mountd      : SSH_HOST : ALLOW
statd       : SSH_HOST : ALLOW
```

This provides a relatively secure file server. Security is ultimately defined by a properly configured SSH server.

Build the SSH Server

This is the login machine that faces the Internet. Given a NAT router, it only shows the Internet one port, 22. Configure your router as such. Once the router is configured, configure a firewall to only allow SSH connections. In RHEL 4, configure the firewall with:

```
# system-config-securitylevel
```

Also configure tcpwrappers for the login host with two simple lines in hosts.deny and hosts.allow respectively. We'll cover additional customization of hosts.allow later.

```
# nano /etc/hosts.deny
ALL : ALL

# nano /etc/hosts.allow
sshd : ALL : ALLOW
```

Now harden SSH by editing /etc/ssh/sshd_config. Uncomment and edit the following lines.

```
# nano /etc/ssh/sshd_config
Port 22
Protocol 2
ListenAddress 0.0.0.0
SyslogFacility AUTHPRIV
PermitRootLogin no
StrictModes yes
PasswordAuthentication yes
PermitEmptyPasswords no
ChallengeResponseAuthentication no
UsePAM yes
X11Forwarding no
PrintMotd yes
PrintLastLog no
Compression yes
PidFile /var/run/sshd.pid
ShowPatchLevel no
Subsystem      sftp    /usr/libexec/openssh/sftp-server
```

PrintMotd should only be uncommented if you are going to use a message as such:

```
**************************************************************************
***                        Proprietary System                          ***
***         Authorized access ONLY. Users subject to monitoring.       ***
***                      ALL other use prohibited.                     ***
**************************************************************************
```

Force sshd to reread the new configuration and we're ready to mount the exported space.

```
# kill -s 1 `cat /var/run/sshd.pid`
```

Mount Export

A few simple operations performed on the login server, we'll create a mount point, edit fstab and, finally, mount.

The exported partition needs a mount point for it to, well, mount. We'll call the new directory, or mount point, /data.

```
# mkdir /data
```

Now make an addition to /etc/fstab for it to automatically mount /data.

```
# nano /etc/fstab
NFS_HOST:/export/data  /data  nfs  hard,intr,rsize=8192,wsize=8192 0 0
```

Manually mount /data with:

```
# mount -a
```

Configure gFTP

Many SFTP clients are available for Linux. gFTP just happens to be particularly robust and user-friendly. It's also more than likely included in any distro you choose. Modern versions of gFTP support SFTP right out of the box.

Enter your external IP address or hostname in the Host box, and your user name and password in their respective boxes. Choose SSH2 from the drop down list on the right hand side. Click the two-computer button on the left hand side to securely connect to your server. Navigate to /data in the right pane. Click Bookmarks->Add bookmark in gFTP's menu bar. Enter a descriptive name and select Remember password if convenience is valuable.

Test and Enjoy

Shut down gFTP and start a packet sniffer. Connect to your server and transfer some files capturing the entire process. After a few transfers, sort your capture by IP address and see if you can see anything that resembles English. I'll spoil it - you won't.

Whithout using it, you can't imagine how convenient it is to be able to backup and retrieve files, securely, at the drop of a hat.

Maintenance

This setup is pretty low maintenance. You could probably just let it run as long as you keep packages up to date. If you're curious or paranoid, you can watch your logs and really see what's going on on the net. Here's a Perl script that mails SSH-pertinent entries from /var/log/messages. Run it at 23:59 each night as a cron job.

```
#!/usr/bin/perl -w

use strict;

# Set date variables
chomp (my $mon = `/bin/date +%b`);
chomp (my $day = `/bin/date +%e`);

# Grep log
my @log = `/bin/grep sshd /var/log/messages`;

# Mail today's log entries
open MAIL, "|/bin/mail -s \"SSH Logs for $mon $day\" email\@isp.com"
  or die "Can't pipe: $!";

for my $line (@log) {
  if ($line =~ /^$mon\s+$day/) {
    chomp ($line);
    print MAIL "$line\n";
  }
}

print MAIL "\n";

close MAIL;
```

Now when you get lots of failed login attempts from farway lands, and you will, add the offending domains or IP ranges to /etc/hosts.allow.

```
sshd : ALL EXCEPT 123. .cn .pl : ALLOW
```

Nothing against China or Poland, those just block all hosts that resolve to those TLDs. It also blocks every IP from 123.0.0.0/8.

To Close

Again, the utility and security of this setup is most appreciated when it's used, and you'll use it a lot. To inject some personal experience, I wrote this article all over the city, writing at a whim, always with a backup.

Remote access can be made even more secure with a key pair and ssh-agent. If your use outgrows your bandwidth, many ISPs have upgraded plans or even business grade service. Who knows what you can do then.

What you will know is that you have secure access to your data. That capability is a valuable advantage in this ever more technologically dependent world.

---

dual is a noob who wants everyone to use encryption, to reduce their ecological footprint, and to spread the antimemes of blackspotting, simplification, and self-sufficiency.

Aminet: The Makeover

This is one even the guys from Queer Eye would loveÖ

By Mobby G

With all the ups and down the Amiga community has faced in its turbulent history, Aminet has been there through the good and the bad of the whole ordeal. Aminet is one of the biggest repositories of Amiga software in the world. With over 5,000 programs and 9 full mirrors, and countless CD releases, it's easily one of the best and biggest resources for your Amiga. Urban Muller, the man behind the start up of this website couldn't be reached for an interview. So hopefully I can give you a pretty full picture of what Aminet has to offer you by way of Amiga software.

First of all, it is always a good idea to use the mirror closest to you. Most of us know the reason why we should, but for those few, who don't, here's why, it can be a little faster and takes some of the load of the main server. I personally used the main server since it was so close, but on those rare occasions it was kind of bogged down or having a problem, I used the one in Germany. Germany seems to be the second fastest from what I can see. But here is a list of the full mirrors:

USA	us.aminet.net
Germany	de.aminet.net
UK	uk.aminet.net
Italy	it.aminet.net
Sweden	se.aminet.net
Norway	no.aminet.net
Czech Rep.	cz.aminet.net
USA	us2.aminet.net

For the complete list, head on over to http://us.aminet.net/info/www/mirrors.html. That will have the above list as well as the partial mirrors. Updates are usually done fairly quickly when new files are uploaded, but if you don't see something on a mirror that is on the main server, just be patient.

On the main page of Aminet, at http://www.aminet.net you'll be greeted by the last 14 days worth of uploads. In recent times, the page wasn't updated as much due to the Amiga languishing in corporate hell. Plus the interface was pretty much bare bones. Now it has gotten a make over thanks to the renewed efforts of Aminet's maintainers. Aminet now stores files for not only the 68K versions of the OS, but for the PPC (OS4, Morph, WarpUp, PowerUP), as well as the i386 based Amithlon and AROS.

There was still some software for the 68K Amiga being written by the community, before the changes, but at only a trickle. Now with the release of OS 3.5/3.9 and OS4, the page is getting updated very frequently. And if you're a music fan, you can always find new mods on Aminet as well.

Aminet is divided into categories to help make finding what you want easier. 15 categories with assorted sub categories allows you to navigate to a specific subject of software you are looking for and allows you to browse what's available. A listing would look something like below...

14Bit_CDPlayer.lha disk/cdrom 92K 1997-12-24 Ver1.1 CDPlayer for Toshiba, 14bit output - (readme)

First up is the name of the program. Most of the files for the 68K Amiga are still in LHA format, and LHA is available in a self executable binary on Aminet. You can also find LHA for the x 86 platforms as well. WinZip allows you to see the contents of an LHA file, but I have yet to manage to get it to extract the files without the actual LHA program being installed. Yet WinRAR seems to have this all built in. Also the x86 version of LHA hasn't been updated in sometime. I would suggest going with WinRAR as it has a GUI and seems pretty solid when it comes to LHA files.

After the name you'll see the directory and sub directory where you found the file. This is if you used the search feature of the site, which we'll cover in a bit, and want to know where the file is located if you decide to come back at a later time.

The next one if of course the file size, followed by the date it was uploaded. Most of the older files have disappeared over the years. I know this from searching for doors and other files for my BBS. But if you have any of the Aminet CDs available to you, these files are not lost forever. You can regularly find them on eBay as well as some of the Amiga retailers online. And since the software on them is mostly shareware, demos and freeware, making a copy of your buddies is probably ok as well. But I would suggest researching this as I didn't have time to for this article.

Now something new has been added, and that is a graphic that shows which platform the program is for. The classic rainbow check mark is the logo for the classic 68K Amiga platform that runs the Motorola 68K cpus (But we knew that already right?). For the new OS4 you would see the red and white checkered Boing Ball, Morph OS would be a Blue Butterfly, and WarpUp and PowerUp PPC would be their respected logos in icon form, as well as for the AROS and Amithlon systems. Then you have a brief description of the program. This is clickable to give you the longer version.

Short	Ver1.1 CDPlayer for Toshiba, 14bit output
Author	flowerpxxxxxx-xxxxxx.xx-muenchen.de (Christian Buchner)
Type	disk/cdrom
Architecture	m68k-amigaos
Download	http://main.aminet.net/disk/cdrom/14Bit_CDPlayer.lha - View contents
Readme	http://main.aminet.net/disk/cdrom/14Bit_CDPlayer.readme

```
A CD-DA player for Toshiba CDRoms that replays via the Amiga audio channels

Version 1.1
-----------

This is an update to V1.0 that has passed through Aminet recently.

*The GUI can now be opened on public screens and when started from a shell.
*Fixed enforcer hits in calibration program.
*Fixed a small bug in sound driver. Sound driver somewhat enhanced.

Features:

* CLI, Workbench and DeliTracker interface
* Previously unseen 14 bit quality.
* Does not disturb and is not disturbed by multitasking (HIGHPRI flag)
* Acceptable (not very high) CPU usage with DMA controllers

* FULL SOURCE CODE INCLUDED!

The CDPlayer is built upon a 14bit experimental CyberSound low level driver. I am having
great plans for a new sound sub system replacing audio.device and sound.datatypes. Drivers
for toccata, maestro planned. Concept texts included! Suggestions welcome.
```

Some of the info not shown here, that is new, is that authors now have the option of uploading a screen shot of the program which will be included on the read me page. Also, some authors like to include the file list for the archive they've uploaded. Other info which is not shown is the distribution of the file. If the author decided he/she didn't want it released on any of the Aminet CDs, they could fill in an optional field in the readme that would let Aminet know what he wanted. The readme is a required file for all Aminet archives, as any file without a readme is suspect to being a commercial program and will probably be deleted from Aminet. Also, some other fields that could show up are "Requires", which would tell you about other archives that the upload needs to work, with a full path if on Aminet. Also memory and chipset requirements could go here. "Replaces" which lets the author specify files that are superseded by this upload. And version numbers as well.

Now if you're in a saucy mood like I am sometimes, and like to just do some searches for keywords or not sure where to look for what you want, the search feature on Aminet is pretty nice and has a few options for you to use to help narrow down what you want.

The search flags are pretty simple. But instead of using the "*" as a wildcard, you would use "%" to match a phrase or keyword. To match a single character, you would use "_". Literals can be escaped with a backslash "\". So as the example on Aminet shows, a search for "lha%." Would return all files that have LHA in the name and before the dot.

One feature of Aminet that I miss that was stopped some time ago was the distribution CDs. Since a lot of their downloads now are from broadband users, they decided to stop. Plus at the time, the amount of incoming software was at a low point, and it didn't make much sense to continue it. But now with the resurgence of uploads, perhaps they will start things up again. But there is a wealth of software on Aminet for your classic Amiga. Hardware hacks being some of the more interesting ones. Just doing a quick look in the hard/hack section you find some very good ones.

2000slot.lha 5K1992-03-11 Use A500/A1000 expansion as A2000 slot
20rom_A1000.lha 2K1996-01-27 Kick20 in A1000 freak's hack
2HDsOn1200.lha 2K1996-08-20 How to get 2HD's on a 1200 or 1HD and a CD Rom
2megagnus50d4.lha 182K 1993-12-04 Build a 2 meg Agnus board for 500/2000
2MegAgnus50d5.lha 183K 1995-10-23 Build (or buy) a low-price 2 meg Agnus board for 500/2000
2Megram.lha 11K1997-02-22 2Meg Ram mod for A500
3to1mix.lha 147K2000-08-28 3 Devices to 1 Mixer
4IDE.lha 14K1998-01-30 Connect 4 IDE drivers to your A1200/4000

So if building hardware is your thing, that is a just a sample of what is there. If you code and still have your Amiga, Aminet is still accepting programs. So why not upload that little app you have sitting there? Or if you have something to make it easier to moves files between the Amiga and PC file systems, upload it. I encourage you to go visit Aminet if you haven done so in a while. I think you'll be impressed with its update and the new software that is now coming out for the Amiga. I would also encourage you, if you do code, to dig out any old programs you have for your Amiga and upload them , or better yet, update them and re-release them. Hell, maybe now could be the time to release the siource code for that little RPG you wrote. Even if you don't code for the Amiga platform, you could always release the source code and have the Amiga Community do the porting.

Well, that's going to wrap it up for this one. In my next one, I'll tell you how to get an Amiga up and running on your x86 based machine using the free WinUAE.

'nuff said...

Hacking the Mirra M-250

By Ustler

Introduction

For some time I've noticed the Mirra M-250 server in stores, magazines, and online advertising. Searching through the web, I was only able to glean basic information about how the server worked. Was it a custom application like the Linksys NSLU-2 or the Linksys EFG-250? What are the hardware specs? Could it be hacked? Was it Linux or Windows based? Did it really perform 128bit encryption like the website claims? These questions and more are what ill be exploring in this article.

Scope of the Article

First off, I want to define the scope of the article (What I'll cover and what I won't cover). Most importantly, this article will cover the basic specifications of the M-250 server along with some information and observations about software, and possible hacks. For legal purposes, I have to remain very vague on some of the contents on the Mirra hard drive (Specifically anything with their strict legal header attached).

Purchasing the Mirra

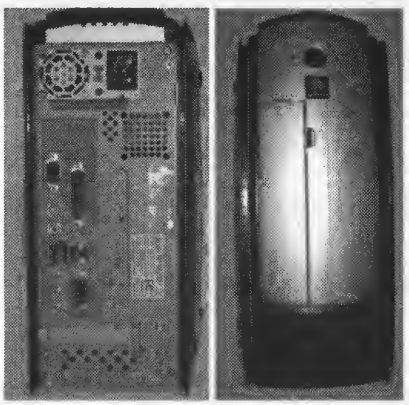
By far, one of my favorite forms of hacking is hardware hacking. For over a year, I've wanted to hack a Mirra server, but never really had the money or time to do so. After much debate, I finally decided to purchase it off EBay for around 300$ (Product was an open box return. MSRP 499$+). It seemed like a good deal since I was getting a 250 GB hard drive (If all else fails, pull the hard drive out).

After waiting a week, which seemed more like months, my Mirra finally arrived. I quickly opened it up and started to mess with it. Since it was open box, it didn't come with any software or manuals, which would normally be fine, but the Mirra client software required a hardware specific cd-key. So for my first hack, I had to do a little social engineering. At first, I decided to play it straight, so I called the company up, and asked them for the cd-key. After explaining where I purchased it from, and why the cd-key was missing, the customer service rep put me on hold and disappeared for 30 minutes. Eventually, he came back and said "Well sir, we are sorry, but we don't support anything purchased off Ebay." So I said, "Well what should I do to get the CD-Key, the item is brand new, but for some reason, the person that returned it didn't return the CD-Key.". And then he made the fatal mistake of saying "I honestly don't know." First off, this really pissed me off. A company should support ANY product that is sold through ANY retailer, and they shouldn't be allowed to discriminate. Furthermore a customer service representative should never admit that he doesn't know an answer. It makes the company look weak and unprofessional.

At this point I was stuck with a useless Mirra server, but I wasn't going to let this stop me. I quickly set up a free email address and created a plausible explanation to why I didn't have the CD-key (Email was chosen because after calling back 3-4 times, I came to the conclusion that the person who I spoke to before was the only person operating the phones) . Without going into much detail, I explained that I had purchased the Mirra server along time ago (6 months), and took out the CD and manuals to read them over. When I finally had time to set it up, I couldn't find the manuals and CD, and went on to explain that I must have misplaced or lost them. I also emphasized that I had spent a lot of my Valuable time looking for the documentation and CD, but was unable to pinpoint their location. After sending this off with the serial code (Which was on the bottom of the Mirra), I waited for around 24 hours before getting a response. And guess what, they gave me the CD-Key (Now how hard was that!).

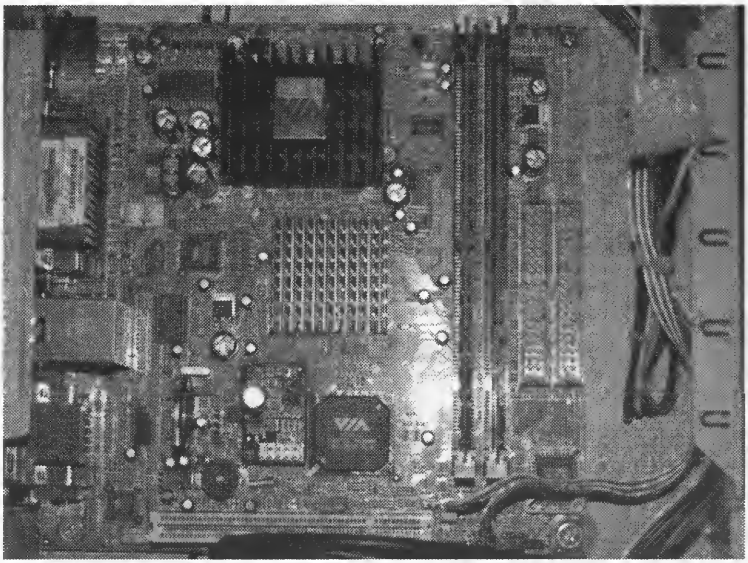
Hardware

Since I had waited for the CD-key for almost 24 hrs, I decided to take a peek inside the Mirra before doing anything else. At first glance, you'll notice that the Mirra sports almost all the input and outputs of a normal PC (Serial, Printer, USB, Ethernet, Sound, VGA). The only things missing are the mouse and keyboard ports.



Outside images

Next, I proceeded to open the thing and scope out the insides. I was able to glean some info from extremetech.com such as "1GHz VIA/Centaur CPU (fan-cooled), 128MB of DDR266" .



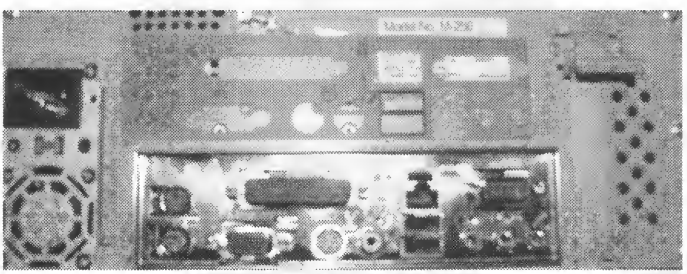
Mini-ITX board fig 1

Just to note, the IDE connectors and front side USB connectors where removed to allow you to get a better look at the motherboard. Also, there is a hard drive just below the PCI slot on the bottom. As you can see, we have all the makings of a normal PC. We have 2 IDE ports, 2 memory slots, a fanless VIA CPU, a PCI slot, and some other stuff. The motherboard is actually an Epia-ESP5000 and the PDF containing all the info can be found on this website (http://www.viavpsd.com/product/epia_mini_itx_spec.jsp?motherboardId=21).

My next goal was to find out the prices for all the components (400-500 USD for the Mirra? How much was Seagate making off these devices?) I went ahead and grabbed all the part numbers off the components and did a quick search on the net for the prices.

Component	Part Number	Cost	Note
Case	CK-1010	45	http://www.casetek.com.tw/mini/ck-1010-1b.htm
PSU (150 Watt)	FSP150-50PL	35.99	No longer sold. It was replaced with newer model
Motherboard with 533Mhz CPU	ESP-5000	98	http://store.ituner.com/ituner/viaep50ed53f.html
Memory PC133 – 128mb	None found	EST. 14.00+	
Hard Drive – ATA/100	ST3250823A	50+	Retail is 108, comes with 50$ rebate.

Now that I had a feel of what I was dealing with, I decided to plug in a monitor and USB keyboard. After hitting the power button, I was presented with a huge Mirra splash logo. Not too long after, the OS started to boot. And guess what, it was LINUX. To be exact, it was Debian Linux 3.0. After the initial boot process, I was presented with a bunch of ReiserFS journal messages (Hmm, guess they're using ReiserFS.) Finally, after 1-2 minutes of loading, I was presented with the login prompt. I quickly grabbed my USB keyboard and attempted to try a few of obvious passwords such as Mirra/Mirra, Mirra/arriM, etc. But for some reason the USB keyboard did not work. Certainly they where preventing any kind of USB devices from working (I would have to guess that they disabled it in the BIOS). Now, according to the manual for the ESP-5000, there is supposed to be a mouse and keyboard port, but unfortunately I didn't notice any during my initial inspection of the peripheral. After taking a quick look inside the box, I noticed that they where indeed there, but for some odd reason, they had covered them up (Security through obscurity!). So I proceeded to peel off the sticker (Shown Below)



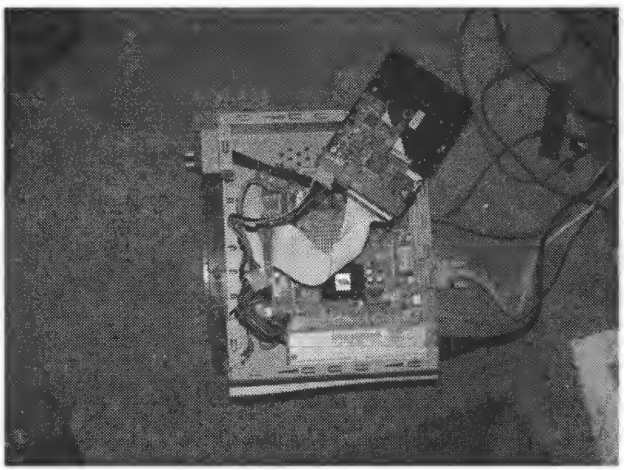
After finding a standard keyboard (non-usb), I went ahead and plugged myself in and began password guessing. Much to my dismay, I was unable to gain any headway in my attempt to crack the password. At this point I had two choices: Remove the hard drive, or find some way to boot of a cd-rom, which leads me to my next section of the article.

Getting the Mirra to Boot

The BIOS on the Mini-ITX board is set up to boot from the Primary Master and any attempt to boot from other devices is futile. Attempting to enter the BIOS gives us the standard annoying password prompt. Now the obvious route of attack would be to reset the bios (Jumper or removing the battery), but in this case, this didn't accomplish anything. After trying both methods, I concluded that the BIOS was a custom OEM build and the password was probably either invalid (Meaning there was no actual password, just a loop for the password prompt) or it was hard coded into the BIOS image. At this point, I really didn't care about recovering the BIOS password; I just wanted to reset the BIOS to the factory defaults. I was able to get the Mirra to boot off another hard drive that contained Linux by swapping the IDE cables (Primary Master), which gave me the idea on how to flash the BIOS. To accomplish my goal of gaining access to the BIOS, Linux wouldn't be the best operating system since most BIOS flashing programs are DOS based. To flash the BIOS, I was going to need either a DOS or Windows Operating system from which I could run the flash program from. To do this, I went ahead and downloaded the opensource alternative to DOS, FreeDOS (http://www.freedos.org/). FreeDOS is very similar to DOS, but it's free, and comes with a lot more features. To make the Mirra boot into FreeDOS, I wasn't going to be able to use the Live CD, so I pulled the Linux hard drive that I had used earlier and hooked it up to another computer I had. After booting into FreeDOS (Via the CD), I went ahead and followed the prompts and installed it to appropriate hard drive. When the installation had finished, I restarted and booted into Windows XP (Which was on the Primary Drive). After Windows finished loading, I went ahead and downloaded the BIOS image and flashing utility and proceeded to save them to the FreeDOS FAT partition.
http://www.viavpsd.com/product/1/0/epia0207.BIN
http://www.viavpsd.com/product/5/0/awfl823b.exe

Next I removed the hard drive and reattached it to the Mirra, making sure to set it as Primary Master. The first attempt to boot into FreeDOS worked, and I was able to flash the BIOS. But for some odd reason, the BIOS still prompted me for a password, so I decided to try the "BIOS reset" jumper again. After waiting a minute or so with the jumper set to reset, I returned it to the default setting, and started to boot the system again. After entering the BIOS, I was relieved to see that the password prompt had indeed been removed. (DO NOT BOOT INTO MIRRA AFTER YOU HAVE FLASHED YOUR BIOS. KEEP READING)

Mirra OS



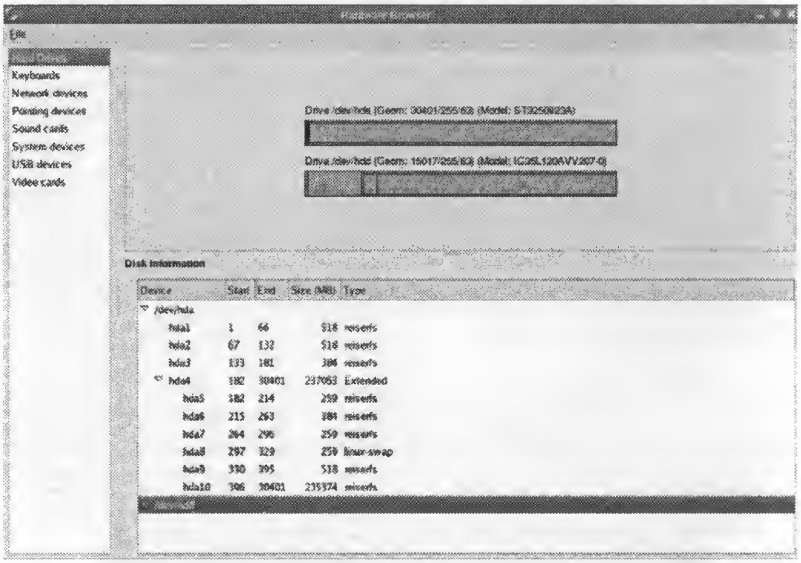
Hacking in Progress

As I mentioned before, the Mirra server is no more than a Debian 3.0 Linux server that's modified to act as a backup server. Of course, it is entirely possible to add features to Mirra without losing any functionality. Samba, SFTP, and maybe even a firewall are entirely possible while still being able to use Mirra itself. To do the following modifications, you are going to need to have done the modifications to the BIOS (If you're booting off of a CD) or the other option is to add a separate hard drive with Linux preinstalled on it (Primary Master), and set the Mirra hard drive to Secondary Master.

Quick note to anyone attempting to boot Fedora Core 4: If you attempt to boot into Fedora Core 4 on the Mirra server, you will not be able to enter graphical mode, and will be stuck with a white screen. This is due to a problem with X11 and can easily be fixed by replacing /usr/X11R6/lib/modules/libvgahw.a
With
ftp://people.redhat.com/mharris/libvgahw.a
Please note this also applies when attempting to install Fedora using the graphical interface. To remedy this, I would suggest installing Fedora from the text based mode and booting into run level 3 to replace the driver mentioned above. Other solutions is booting into runlevel 3 and running

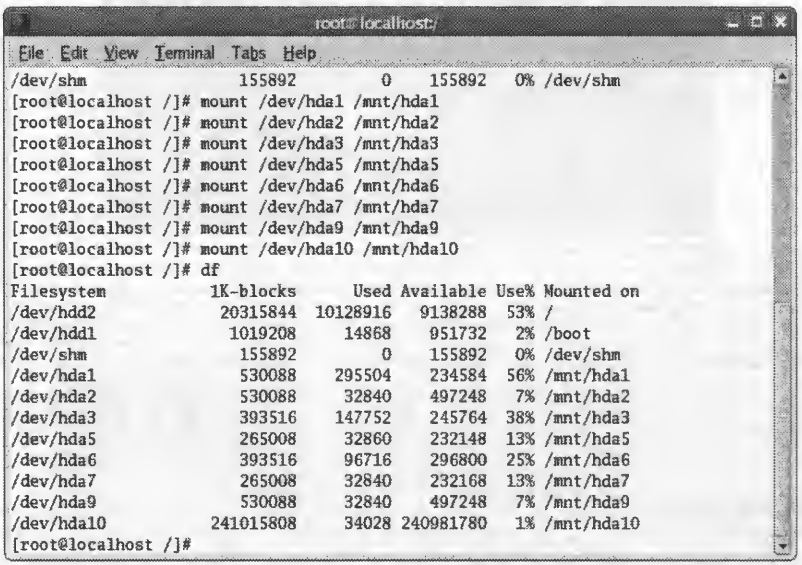
To explorer the Mirra hard drive, I'll be using Fedora Core 4.

First let's look at the layout of the Mirra hard drive:



First thing we notice is that there are 3 primary partitions (hda1, hda2, hda3) and an extended partition (hda4). Within hda4, we have 5 reiserfs partitions and one swap partition. The next task is to create folders to which I can mount the partitions to. This is pretty simple, just do
mkdir /mnt/hda1

And increment the number at the end till you're at 10 (Excluding hda8 and hda4, which do not need to be mounted). Now where ready to mount our partitions (Shown in the picture below)



Mount Points Breakdown

Partition	Mount Point
/dev/hda1	/
/dev/hda2	/altroot
/dev/hda3	/var
/dev/hda5	/ispiri
/dev/hda6	/update
/dev/hda7	/tmp
/dev/hda9	/slop
/dev/hda10	/data

Since we have the partitions mounted, we can now explorer the contents of the partitions. The first partition we are going to look at is hda1, which is the root partition. Inside hda1, we see the usual allotment of Linux folders, but take note of the following folders since they appear to be out of the ordinary. These folders are altroot, data, ispiri, and slop. My first impression about the folder "altroot" was it was used to chroot, but this is not what it's used for. Altroot is the mount point for hda2 and is used for updates. Essentially, in the case of an update (Major), the Mirra server would download the files and extract them to altroot. Then it would set lilo to boot from hda2 instead of hda1, hence swapping the partitions (This may not be entirely true, after I figured out that it was not using altroot as a chroot directory, I decided to stop investigating it.)

Probably the most important part of hda1 is the /etc/ folder that contains the rc.d files for booting. These are the files that we will need to modify to ensure that we are able to boot from the Mirra hard drive without messing up our BIOS image. In particular, you need to find the file "S18ispiri-bioscheck" (Please note this is a symbolic link to /root/init.d/ispiri-bioscheck)

find /mnt/hda1 -name S18isiri-bioscheck

In my case, I just moved the file into /etc to prevent it from running. The file itself is pretty simple. It creates a SHA1 hash of the nvram, and if it doesn't match the one contained in the file itself, it will restore the nvram from "/ispiri/nvram/slurpee/lastnvram". Most of the customization scripts are contained in /root/init.d. One very important thing that you might want to note about the boot process is that the lilo.conf contained in /etc is not used. If you look at /root/init.d/ispiri-setup you will see that lilo.conf is removed and a symbolic link is placed to /root/lilo/lilo.conf. This same file also contains the script to migrate from hda1 to hda2 during an upgrade, just in case you want to look for yourself.

Now that we looked at hda1 and hda2, we can move onto hda3. This partition is your typical /var so there really isn't much to notice. The only thing worth noting is the "ispiri" folder that contains some files in a subdirectory called slurpee. Taking a look inside of the file client.db, you will notice that its formatted in XML. Most notably the value <RSAKeyValue>, which makes me wonder if they are implementing some sort of PKI system running on their servers.

Surprisingly, hda5 is an exact copy of /var/ispiri/. This is probably for backup purposes, although I could be wrong. On the other hand, hda6 offers us a complete backup of the Mirra OS. I don't know if this is particular to servers that where upgraded, or if it's common to all Mirra servers. It would make sense to keep a complete backup just in case the system became corrupt or problems started to arise. Within hda6, which is mounted as /update, we have two folders, osload and precious (Must be a Lord of the Rings fan). The folder precious has one file names license.xml. This file appears to contain some interesting information. As the extension applies the file is in XML format and contains only three values; licensekey, securitykey, licensekeystate. The LicenseKey value, as its name implies, contains the license key used to activate the software. The Security key on the other hand is probably associated with Mirra.com servers. The last value is used to verify the state of the license. For example, in my XML file, the value is set to $VERIFIED, which probably points to another value set by one of the startup scripts.

Now that we briefly examined the license.xml file, we move onto the osload folder. This folder contains the root files in gunzip and cpio format. The file control.xml has the names of the files to extract along with the SHA1 hashes. The extraction process is pretty straight forward, so we wont cover exactly how to extract or manipulate these files, if you need assistance with this, contact me and ill get back to you.

The hda7 and hda8 partitions are standard on most Linux systems (/tmp and swap) so we won't discuss their purpose. Last but not least, hda10. This is the actually data partition that Mirra stores the backup files on. As shown in the previous table, the mount point is /data. The Mirra program itself doesn't actually access the /data directly, but through a symbolic link contained in /ispiri/slurpee/. It is entirely possible to mount an extemal drive and repoint the data partition, but this would require editing the startup files (Which reconfigures the symbolic links during startup)

Hacking in Progress with the CD-ROM and secondary hard drive

All right enough with looking at the layout lets start working on gaining root access. After attempting multiple different methods, I came up with an easy solution for changing the root password. To do this, we need to change the default runlevel to one. Next we are going to need to mount the hda1 partition and modify /etc/inittab. Now, any Linux guru would probably wonder why we wouldn't attempt to replace the lilo bootloader, and then append the runlevel. The answer is actually simple, unless we modify the inittab file, we won't be able to log into the box without a password.

Normally single user mode would not require a password, but in this case, we have an additional line added to our inittab

~~:S:wait:/sbin/sulogin

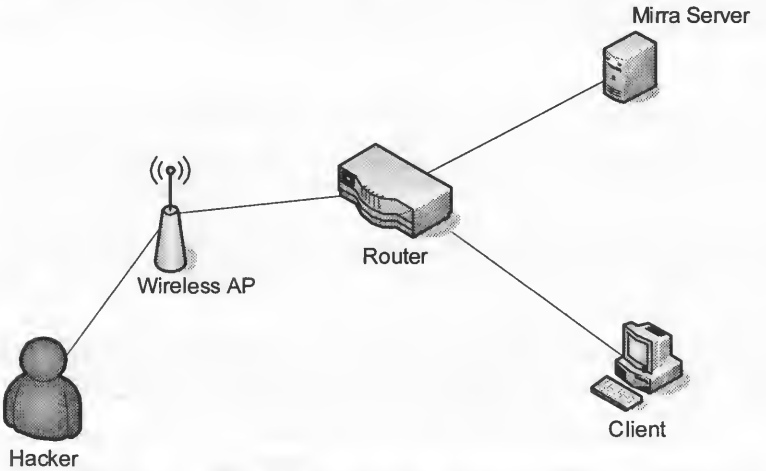
This entry is used to require a password for runlevel 1. To defeat this security measure, simply comment it out with a #. After commenting that line out, head up to the line just below "# The Default runlevel.". Here we can specify the default runlevel. Normally this would look like "id:3:initdefault:", bu we need to change this to "id:1:initdefault:". After rebooting, you should be given a shell with root access. Now its time to change the root password. This is rather simple, just type in "passwd" and change your password, simple as that. If you are running the client software you'll notice that the connection to the server isn't present. To get the server to work with the client software we need to change to run level 2. Before we do this, there is one important file we need to remove. These are /etc/nologin and /etc/nologin.boot. These files prevent logins from the console and are re-added through a startup script every time you boot. After removing them, we can enter "telinit 2". After this, we have to wait 1-2 minutes for it to switch runlevels. After it's done, you should be able to type in the username "root" and the password that you entered earlier. Great, now we have console access, what about SSH? Well, SSH access has a few tricks we need to employ to get it to work. Normally in runlevel 2, the script S19-ispiri-sshdebug would run. In the startup script, it checks for a variable that defines whether or not the server is set in debug mode. If its not in debug mode, it a file is created in /etc/ssh/ called "sshd_not_to_be_run". If this file exists, SSHD won't run. Simply remove this file also. Now we go back to /etc/rc2.d/ and run "./S20ssh start". And it's as simple as that.

Putty connected to Mirra

Server and Client

We haven't talked much about the server/client part, so we will briefly talk about it in this section. As you may have noticed, Mirra runs on Linux and the client is based on Windows .NET (Weird Combination). The actual server part is built in Java and runs on Jetty, the 100% Java server. Since I don't program in Java, I'm not even going to try to figure out how it runs, and ill leave that up to the Java nuts. What I do know is the server is vulnerable to a denial of service attack (Determined by scanning with Nessus) [http://secunia.com/advisories/11166/]. Other than that, nothing else appears to be remotely exploitable. Now I wanted to take a quick look at the way the server and the client communicate. According to the site, the server uses 128bit SSL encryption, but the keyword that made me suspicious was "internet". Now anyone with any background in networking knows that there is a big difference between internet and a LAN. What I wanted to know was whether or not information being transferred from the Mirra client and server was encrypted. For the client to work, it has to be on the same network as the server, so I had to assume that the connection was not being tunneled through a proxy of any

sort. Running ethereal produced some very interesting results. The authentication key appears to be generated from Mirra.com and is sent to the server by the client in clear text. On another note, the client sends all the information in friendly and unencrypted XML. Now, being of the curious nature, I've done a little war driving around Doctors Offices (One of the Primary Clients for the Mirra Server) and have noticed that most of them either don't encrypt their wireless LAN, or simply use WEP. Since the Mirra sends information Unencrypted over the LAN, and only encrypts data when it's being accessed via Mirra.com, it's entirely possible to either sniff the traffic (If the client part is wireless based) or attempt a man in the middle attack. Just in case you're not familiar with a Man-in -he-Middle, ill give a quick example. First off, our network layout is below. To employ this hack, we use a technique called ARP Poison Routing (APR). This technique relies on the fact that the ARP protocol does not use any form of authentication and is stateless. Essentially what we are doing, is re-routing the traffic from the client through our computer before it reaches the Mirra server. Normally this could be solved with a layer of encryption (Such as SSL), but unfortunately this feature is not implemented. I know there are a variety of ways to protect against a man-in-the-middle attack, but SSL seems like a quick and easy solution for Mirra when deploying a server in an unknown environment.



As we mentioned before, the authentication appears to be some sort of public key system for authentication, thus eliminating the ability to do a Replay attack. What you may be able to do is a connection hijacking/spoofing attack. In this attack, we would first monitor the communication using a sniffer (Possibly ARP poisoning depending on the topology), after we have enough information, such as the authentication credentials, we attack the client with a DOS or similar attack to disconnect the client (In a wireless environment, we would force the client to disassociate). While we are doing this, we can replay the traffic and impersonate the client (With appropriate spoofing, of course).

Another weakness that I've identified was the fact that it sent out "sleep" packets at a set interval. These packets are in XML format and since they are at a consistent rate, it leaves open the possibility to perform a "Known Plain Text Attack" when dealing with cryptography. If a LAN is being encrypted with certain algorithms, we can collect these packets (Which are at a consistent interval, hence we look for packets at that interval over a period of time), and eventually determine the key. The only form of randomness is the time and date, and even that can be guessed.

Expanding the Possibilities

In my opinion, I would rather just run Linux off the hardware rather than using the Mirra modified version of Debian Linux. Although most of you hopefully feel the same, some of you might want to be able to use Mirra.com and be able to access it via SSH, FTP, SFTP. Well fortunately for you, I do have some suggestions. I do have to warn you that certain upgrades (Such as Perl) will break the Jetty server (Can be fixed by moving libraries around, or downgrading). Also, if memory serves me right, the Mirra already had apt-get installed on it. The only problem was that the directory structure was missing. So after re-creating the directory structure and adding the proper sources, I was able to successfully run "apt-get update" and the "apt-get install nmap" or "apt-get install gcc". I would highly advise against running "apt-get upgrade" because it will break the Jetty server (Perl upgrade). On a further note, you may have to play with a few things to get it to work. We won't discuss this

since this is only an introductory article on the Mirra server and the fact that I have space and time constraints. I can say that I've successfully installed vsftpd, openvpn, nmap, nessus, and a few other tools.

Vast Room for Improvements

Seagate has a great idea, but really needs to improve the security of their product. Of course they won't be able to "Totally" secure the backup server, but the current security when transfer between client/server is weak. Also, I would like to see them implement encryption when storing information. Now you may wonder, wouldn't that be expensive and require a faster platform? Well fortunately with VIA's new PadLock technology, this is entirely possible. VIA PadLock is, to my understanding, a hardware based encryption mechanism able of performing AES encryption acceleration. Check it out (http://www.via.com.tw/en/initiatives/padlock/hardware.jsp). We can clearly see from the comparison on the website, that the PadLock technology effectively reduces the encryption time significantly while using less CPU utilization. Also, a Trusted Platform Module for storing passwords and encryption keys along with a way to securely backup the keys would also be appreciated. Of course I understand that these security features could raise the price of the product, thus I would suggest the ability for a purchaser to customize the appliance, or upgrade it. For example, you could buy the server at Best Buy, and then pay 100 dollars to upgrade it to a high security model which would require some sort of hardware addition.

Closing Thoughts

While Seagate and Ispiri have done a relatively good job at bringing a backup server into the market, much is to be desired when it comes to security and pricing. Not only, in my opinion, is the product overpriced, but it lacks the features that would allow it to crush the competition. Of course the feature of "Remote Access" is to be desired, but we are dependent on Mirra.com and Seagate for their services. If Seagate ever decided to close the website down, we would no longer have remote or local access to the backup server. While this probably wont happen anytime soon, I fear that it may be discontinued down the road due to lack of sales. As for pricing, I feel that Mirra is extremely overpriced. The price differences from the M-250 and the M-160 is over 100$. That's 100 USD for 90 gigs of extra space. May seem reasonable to some, but you have to consider that the actual hard drive is an ATA/100 and the MSRP is approximately 50$ after the mail in rebate. Furthermore, the price between the M-400 and M-250 is 300 dollars (799$ and 499$). Considering that I could simply purchase a second hard drive and mount it in the spare 5.25 slot (Thus giving me 500 GB), I doubt the price is raised with the cost of hardware. In conclusion, I feel the Mirra is appropriate for small businesses lacking technical expertise, but for the rest of us, don't waste your money. Might as well go buy the hardware yourself, and install Fedora.

Warning: Modifying your Mirra server may void your warranty or cause you to loose service with Mirra.com. Blacklisted 411 Magazine and it's staff does not take responsibility for your actions and does not guarantee that these methods are safe. Blacklisted 411 Magazine is not associated with Mirra.com in any way.

CLOAKING AND YOU

By Grandpa Hackman

It sounds so mysterious. Cloaking. Like something with ominous gray overtones.

Why is it done? How is it done? What is the future of cloaking?

This article will attempt to answer those questions.

I won't be able to include the actual instruction booklet to tell you how to cloak, but I can tell you what it's about, and how to find out more. Also, this article describes website cloaking, not the kind often used by hackers to hide themselves for roots. To fully understand what it's all about, an explanation of search engine optimization is in order.

Priorities. That's what it's about. Money. If you're a website owner, you have many options available to you to advertise your site. Advertising your site is essential. After all, you may have the finest mousetrap on the planet, but if nobody knows about it, you're not going to catch any mice.

There are not as many options as "the good ole days", but there are still a lot of methods to advertise. There are "surf engines" like ts25 (one of the best for the buck), double-opt-in safelists, pay-per-click, etc. If you're hyping a website, you probably use all of these options and then some.

But it's hard to beat the "targeted traffic" you get for free from a search engine. Or should I say "You can't beat the targeted traffic you get for free from a search engine." This is because your potential customer came to you actually looking for your product. He's 80% sold before he gets to your page. He needs and wants this widget and actually went to the trouble to search for it.

And not only is this a very special customer likely to buy, buy, buy, but it didn't cost you a dime. Most other methods have some cost involved and on top of that, the customers are not "targeted", they just happen to be interested in the subject line of your email or your pretty webpage struck their fancy as it flashed across their screen, etc. They still don't know that they want or need your product, they're just temporarily mesmerized. Now it's your job to "sell" them your product, much tougher than just supplying what they're already looking for.

OK, so now we've discussed why you would want to be listed on the search engines. What is involved in getting listed?

Well, with most of them, not a whole lot. Yahoo wants $299/yr. to "think" about listing you, no guarantee you'll get listed, what a deal. Fortunately, there are ways to "trick" Yahoo into listing you without paying that outrageous graft.

But most of the rest will find you with their spiders. Now, this can take months. Most site owners are a little more anxious than that. Again, there are ways to speed up this process, for free even. Well, it involves effort on your part, but at least no capital outlay.

And then there is the issue of ranking. It really doesn't mean much if you get listed on a search engine and you're back on page 68. Nobody is going to see you, NOBODY.

So not only is it important to get listed, but it is mandatory that you get a good ranking. Otherwise, your goal of making money is not going to be realized.

Google states on their information pages that: "Google doesn't accept payment for inclusion (known as "paid inclusion") of sites in our index, nor for improving the rank of sites in our results."

This appears to be the case. Google claims that their ranking system is based upon "a complex algorithm" designed to prevent fraud and designed to give ALL the opportunity for a good listing, regardless of financial clout. All well and good. Then they go on and tell you "It's also possible that we're not able to crawl your site due to technical reasons. A few of the most common ones are listed below:

- Your pages were unavailable when we tried to crawl them.
- Your pages are dynamically generated.
- You employ doorway pages.
- Your pages use frames."

And that's the problem. Except for the 1st instance, you may very well be employing one of those methods and have trouble getting listed. And you probably have very good reasons to write a dynamically generated page, for example. These tend to be infinitely more work to produce and for all your labor, you are rewarded with a page that Google won't list.

Which bring us full circle to cloaking. Cloaking is a method which allows you to serve one set of pages to the search engines and another set to humans. Or other divisions according to data sent by the requestor. Here's how it works:

When you (or the search engine) request a page an "http header" is sent. Here's an example of the information in this header:

GET: /index.htm
HOST: www.yoursite.com

USER_AGENT=Mozilla/4.71 (Windows 98;US) Opera 5.50 [en]
REFERER=http://some_refering_site.com
REMOTE_ADDR=123.122.111.006

By watching the user_agent and/or remote_addr fields, you can dynamically produce pages styled to the viewer. By keeping simple lists/databases of the known major spider ip ranges you can easily pick them out. In the case of a search engine, you give them what they want, a page optimized with keywords, no frames, etc. In the case of the humans, you give them what they want, a spiffy-looking, easy to navigate page. It's a win-win.

The search engines all claim to abhore this technique, but they won't absolutely ban it because they'd have to dump the most profitable pages they have.

There can be many reasons why you would want to work in the gray area of cloaking.

You can use cloaking to serve appropriate pages to unique regions of the globe. Or have one set of pages for dialup customers and another set for broadband visitors. Many various reasons.

SearchEngineWorld has a great forum on "search engine spider identification". At that site you can find the ip address range of most of the major spiders. And many other interesting facts.

If haven't made cgi pages before, you can learn to make pages that feed data out according to criteria obtained from the requesting party. There's software for sale that claims to do the cloaking for you.

It's also interesting to note the number of "unknown" spiders that are out there, and seemingly up to no good. Really, they're up to something, but what?

Four of the most basic and common methods of cloaking are: User Agent, IP, IP Delivery and IP Redirection.

User Agent: This is the simplest form of cloaking. Most major search engines set the user agent variable to the name of their search engine spider. They also put the word "mozilla" in their user agents to "fool" you into thinking that a Netscape or IE browser is hitting your site. You can easily write a script that shows the cloaked page if mozilla is absent and deliver optimized html if it recognizes a spider name.

IP Cloaking: Most web servers have a RemoteAddr variable that allows you to check the IP address of the site visitor. Using a list of known spider engines you can write a script that identifies a spider by it's IP address and deliver html that is designed for exactly that spider.

IP Delivery: This actually describes the method of delivery of html when you have determined whether you are dealing with a spider or a human. It simply serves up the appropriate page on the spot.

IP Redirection: In this method, the "spider page" IS the initial doorway page. If it is indeed a spider visiting you are done. Otherwise the requester is redirected to a page designed for humans.

There are many outstanding resources on the web to guide you towards effective cloaking. You should also be aware that at least publicly, the search engines frown on the practice of cloaking. For this reason if you are caught doing it you may be penalized. For example, Google will lower your page ranking. Some search engines will expel you from their database. So if you do decide to cloak, don't get caught.

Learning to cloak websites is a mighty contribution in the hackers bag of tricks.

Hardcore Wardriving

SANITY IS TEMPORARY, GLORY IS FOREVER

By Israel Torres

This article is not for the faint of heart and the situations explained herein are real. Names have not been changed to protect the innocent. Facts have not been obscured in any way.

Introduction

Before we continue there is one thing you need to fully comprehend. Wardriving is not about committing acts of crime, or connecting to Access Points you find in your wardriving adventures. In fact you really shouldn't be interested in the details of your logs until after you have completed your wardrive. Already confused? Wardriving is best explained by this well known statement and definition of what wardriving is all about:

"*WarDriving v. The benign act of locating and logging wireless access points while in motion.*" - blackwave

Let us break this quote down to get a full understanding of this term that is misused to this very day by parties worldwide.

"*The benign act*": This means that the action itself is not meant to cause harm in any way. Harm as in trespassing, violation of privacy, or anything else.

"*of locating*": This means that by using a (Global Positioning System) GPS unit you know *exactly* where on the planet Earth you detected the wireless access point's signal at any one time.

"*and logging*": This means that after you locate where on the Earth a signal was detected it is then logged into an artifact for later analysis.

"*wireless access points*": These are commonly known as APs, and are what are sending out signals far beyond the holds of any physical barriers. They are not limited to WiFi.

"*while in motion*": This gives into the driving part. Be it * as in driving, walking, biking, flying, rafting and all the other creative war[something] out there. The key idea here is that you are moving and not parked anywhere or in a static position.

So just to make it clear wardriving is completely legal (at least in most parts of the free world). If people don't like it they shouldn't be using systems that cross physical barriers and into to free space. In short, wardriving is not a crime.

Ok, we really had to get that out of the way so that when wardriving is being referenced there can be no confusion as to what exactly I may be talking about. If you are still confused ask someone to read this article and then explain it to you. I also hope that this quick piece of education will clear up all the nonsense out there that continues to cause havoc to this day because people don't know what they are talking about. Learn it, love it.

The Facts

Here are some facts that I will let you in on so that if you do choose to wardrive you can get an early grasp before spending a grip of cash (or credit) on your wardriving hobby. Many bait you by just saying you need a wifi card for your non-wifi enabled laptop. This is where the journey begins because it all sounds so easy.

To the outsider wardriving is boring. I mean really really boring. If you look at it from a non-hobbyist view you are actually driving around with nowhere to go – what is the point of that? A wardriver hovers to a destination area usually composed of several miles and then leaves, rarely with even stopping the vehicle – and never leaving a trace. No sir, if someone doesn't get a taste for wardriving the first time around, they most likely never will. In fact in my adventures I try and ask a person to take the role of a navigator (one who assists with the map reading and overall navigation of the "mission".) but rarely are they focused on the screen (I have learned to memorize my routes). I have come to understand they are there to chat with and keep one company. You may try and explain to yourself this is not true but in the end it really is. 98% of my wardriving is done alone, and mostly for the fact that finding someone to join is often most difficult especially if they have done it with you a few times. There are some wardrivers that cope with this "*non-destinious*" by creating a destination to wardrive to. This helps the mind cope with the fact that you are wardriving. For example say you haven't done an area in Los Angeles and know for a fact that no one else has taken credit (on WiGLE) for it but don't want to traverse 100 miles out of your way just to wardrive (that would be crazy). So you tell a buddy, hey let's check out Downtown LA's districts and see if we can find cool deals on stuff. If your buddy agrees then the guise is working and you are in good shape. They see you fooling around with computers and wires and ask you what you are doing. You can get away for the moment by explaining in half-truth that you are setting up the GPS navigation system. Unfortunately it may start to fall apart the minute they ask why you aren't taking the freeway there. One hour turns into two and next thing you know they appear to be livid over this whole trip. They will certainly be most careful next time you query them for a trip in the future.

The time spent wardriving really depends on your dedication to the hobby. After all it is just a hobby. There is no method to extract dollars from this hobby. Especially nothing profitable when taking into account the miles put into the vehicle, the gasoline alone could break a wallet in two. Most important is the time. If time is money and you are wardriving then logically you are making negative dollars per minute per mile. I have wardriven a 24-hour wardrive without a break other than to eat and let me tell you it is rather maddening. More recently I have shaved my wardrives down to a few hours; timed perfectly for "traffic windowing". This allows me to get into a target destination and fill my logs then get out before the flow of traffic drastically changes into a nightmare. I have found this to be most adequate for yield over miles. I have spent thousands of dollars in gasoline fuel and vehicle maintenance alone in this hobby.

Ok so we wardrive and log stuff. What do we do with the resulting stuff? Personally I am an advocate of WiGLE (Wireless Geographic Logging Engine) (http://www.wigle.net) and upload my daily logs and declare that all wardrivers should do the same. If you don't that is ok too (but then brother, you are really wasting your time). I came up with the motto: ***"Log them all... Let WiGLE map them out!"*** In my days I have learned a few tips (mostly not known to all – until now) to get the maximum out of your wardrive logging. With NetStumbler use the fastest scanning speed (yes you create larger files, but are going to miss less), and with Kismet you want to upload all 3 accepted files (xml, gps, and csv) I hadn't done this when I began my adventures and then learned that all files combined contain different information and could potentially account for 10-20 percent of the logged networks you may be missing out on if you don't upload all 3. Just do it and you will be pleased with the results?

One of the least important aspects (within the scope of wardriving) is the hardware. Sure anyone could put together a decent wardriving rig for a few hundred dollars and a laptop. All you need is a WiFi card, external antenna and gps unit to get reliable logs. It is the time spent researching and configuring that will take its toll. After you have the "perfect setup" you really won't need or want to touch it again. You know that the minute someone is updated and you try to reconfigure your wardriving system something may break and you could lose a few days fixing it. Those are valuable wardriving days we are talking about. My suggestion to you is build an independent wardriving system and then just use it for wardriving. I have seen countless people try and have an all-in-one system where they can use it for general things. This is a waste of time. Take my advice if you are serious.

Next that comes into play is the software. Once and for all I will bring it out loud and clear. **If you aren't using Kismet (or something kismet-based) then you are wasting your time.** This fact is plain and simple. You can argue up and down all day how useful a NetStumbler-based system may be handy for everyday Windows users but I can tell you right now if your sole wardriving system solution is using NetStumbler then you might as well shoot yourself in the head. I will not go into the specifics of why, because you most likely could care less. It is fact, get over it. If using Linux scares you it is time to evolve. Learn it, Love it.

After the "you-can't-get-enough-but-need-to-get-more syndrome" hits you start looking for shortcuts (faster ways of getting more APs per less mile); answers to more questions as it were. You start to question the power of the ORiNOCO Classic gold – the de facto wardriving card that works both in Linux (for kismet) and Windows (for netstumbler), heck it even works for Macs (for macstumbler). You start to question your antenna's dB/dBi and want more. You no longer care what your vehicle looks like from the outside or that your drag coefficient has destabilized due to the number and types of antennas you now are armed with. You throw money at amplification units to give you that 10% reach into the digital ether, grasping at quiet beacons, begging them to come near. You want more. It is a never ending thirst. You have become a WiFipire.

The Conclusion

Ok so at this point you are wardriving and uploading your log files to WiGLE. You hear kismet whistling in your sleep, and you feel alone when no such sounds exist.You are spending a whole lot of money on gas and vehicle repairs. You have lost friends and gained competitors (from those that liked the wardriving experience). Your interest is mainly staring at maps and memorizing optimal routes. Everyone and their mothers have AP-envy and all you can do is smile and tell them to say your name. Yes, friend you have joined the circle of the few, proud and insane. It is lonely at the top. Your mission is to claim and reclaim positions on the WiGLE's ranking. Your goal is to become the undisputed hardcore wardriver. There are no boundaries you cannot overcome. The uneducated fear you and call you names. Your hobby is a hobby like none other.

Personally I have a number of dedicated wardriving systems that I have built. I truly enjoy wardriving as I have explained it above. I have been called various names and even "*amateurly*" diagnosed as having a compulsive disorder because I enjoy this hobby and strive to be the best. People can talk all they want; it is the action that becomes history. As of this writing within less than 90 days I have reached around 200,000 logged access points with GPs coordinates. I am very lucky to be in an area that is known to be high-density as well as technologically enabled. Most are not and therefore my advantage is topped with persistence. If you aren't aware already I am currently at WiGLE's second ranking with full intention to claim first ranking soon enough.

The mother of all wardriving related questions is this:
"Why do wardrivers wardrive?"
In the end there is no universal answer other than "because we can"

When someone asks you where you are going you can tell them you are going crazy.

DEFCON 13

A RECAP OF THE FINEST HACKER PARTY ON THE PLANET

By Electra-Solve

It was an honor for me to cover DefCon 13 for Blacklisted 411. It's the premiere hacker underground event, there's nothing else quite like it. For those of you that haven't made it yet, it's full of skullduggery and stealth, sheep and the wolves that prey upon them.

But don't dwell upon that darkness, it's all in fun (sort of).

The Alexis Park Hotel in Las Vegas hosts the convention.

DefCon is a no man's land where federal agents and free thinking hackers are supposed to share ideas to make people safer. But it is really a showcase where hackers can "strut their stuff." For that type of person, it's hard to beat the $80 registration for 3 days of fun.

For one thing, it's a great place for security experts to demonstrate their prowess to others that can comprehend the ramifications.

Or it can be for hackers skilled in one or many of the facets of hackerdom to demonstrate their knowledge. Contests abound. The subjects are as varied as lock picking to war dialing.

Or for those who'd rather listen to someone knowledgeable speak, there's plenty of that too. Speakers this year included Phil Zimmerman of PGP fame. The Assistant Secretary of Defense for Networks and Information Integration, Dr. Linton Wells II was another big one. The Feds. There are speakers on scores of subjects relating to hacking and security.

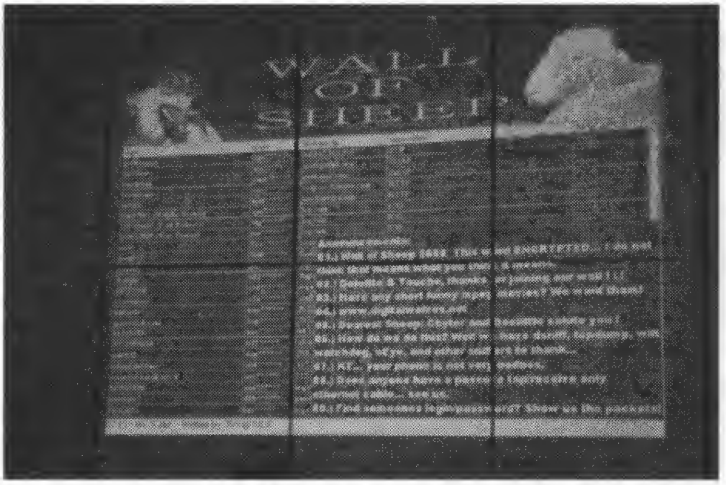
Then there's the demonstrations also, sometimes from vendors trying to get you to purchase their wares, other times the latest greatest wizards showing a major weakness that can be exploited if it's not fixed. And how to protect yourself from those same flaws.

Swag giveaways galore. You get enough t-shirts and hats to last you for years. As you walk down the aisles it is literally shoved at you, you can't walk out empty-handed, no matter how hard you try.

And the vendors are there in force. From book vendors selling anything from "How to Pick a Lock" to "How to Make Drivers Licenses and Other ID's on your Home Computer." There was several tons of old computer hardware for sale too, neat stuff. Some not that old, I saw many laptops going for give-away prices.

But it's Vegas too. So there's plenty to keep you entertained no matter what you're doing. I hung out a lot at the pool when I wasn't attending DefCon, I mean, it's the Mojave Desert in the middle of summer! For those of you that enjoy alcohol, I don't have to tell you that Vegas & booze are almost synonymous. Even the pool was fair game though, soon sporting purple water, is nothing sacred?

Unlike many conferences run in Vegas, this one has a lot of user participation. Uh, not always intentional. Using any unsecured wireless access, like the hotel system, was foolhardy. There was a large public screen displaying the infamous "Wall of Sheep." Those who were brave enough to use one of the many wireless networks available without using a VPN or SSL had his username and part of his password appear on the screen for all to see. Not a sought after goal, needless to say. Other details too. At least one poor fellow was careless enough to use an unsecured webcam on the hotel network. He got to see his face plastered on the "Wall", with the caption "Have you seen this sheep?"



The "Wall of Sheep". If your username appeared here you became entertainment for the crowd. And part of your treasured password became compromised.

Among the exposed sheep were an engineer from Cisco Systems Inc., multiple employees from Apple Computer Inc. and a Harvard professor. Would that be the same Cisco Systems that tried to silence a whistleblower that discovered security flaws in their routers early in the conference? Yep. Who says these guys aren't security conscious?

Fortunately, I had a heads up from friends. I was very leery and avoided all wireless networks there personally. It turns out I did the right thing. At the awards ceremony on Sunday, the organizers of the conference mentioned that they had checked and there were at least 130 wireless networks set up around the conference, all with the aim of luring in suckers to pass their usernames & passwords across these unsecured networks.

The annual "Meet the Feds" panel was a hit again this year. That's right, the boys from NSA, FBI, Treasury and Defense Departments attend with a presence, it's said that much recruiting from the hacker ranks occurs here. The panel members said that they would love to hire the "best and brightest" hackers, but made it clear that they would not consider those that were lawbreakers.

This has prompted the ever popular "spot the Fed" game. It's pretty simple. You and your buddies go around trying to ascertain who looks like a Fed. Then you ask them. Rumor also has it that they will fess up when questioned. This year they were handing out T-shirts to the winners that said "I spotted the Fed!" They also gave one to the Fed caught red-handed "I am the Fed!"

Robert Morris Sr., former chief scientist for the NSA (!?) gave a lecture on the vulnerabilities of bank ATMs. He made the prediction that they would be the next "pot of gold" for the hacking community. He then went on to give examples of scams that had already been pulled in an attempt to compromise people's ATM security.

He said thieves have been able to gather bank card information and passwords by modifying the software in used ATM machines bought off of Ebay. The machines can be purchased for as little as $1000. They are then placed in public places like a mall where unsuspecting users attempt to access them. The machines accept their card and ask for their PIN number. After they enter the PIN, it spits their card out, saying that funds are not available. Meanwhile, it stores their card information along with their password. This can be used later to drain money from their account.

At one point in the lecture, Agent Jim Christy asked everyone in the audience to stand up. After they did he said "Now those of you who haven't broken the law-sit down." Many did, but others did so with a lot of hesitation, one might say with body language stammering. Eventually everyone sat down. He then joked "OK, you can turn off the cameras now." Those crazy Feds, they're a laugh a minute.

Dr. Wells also spoke on recruitment: "If you want to work on cutting-edge problems, if you want to be part of the truly great issues of our time... we invite you to work with us."

Uh, ok.

Phil Zimmerman, creator of PGP also spoke at the conference, hyping his new VoIP encryption system. He stated that the Internet had become a "crime ridden slum."

His device installed on the client phone side and is called zfone. It is based upon Shtoom, a Python program, and it too is written in Python.

It then produces unique codes to that user, setting up an encrypted, secure connection.

Most VoIP security systems tend to use a central certificate authority. Phil Zimmerman thinks it's too much trouble to set one of these up for something as simple as a telephone call. His system is much simpler, with no central login needed.

One thing's for sure. Whatever Phil Zimmerman decides to get involved in has a good chance of being a major winner. So I'm keeping my eye on this one. Besides, it occurs to me how insecure VoIP data is. Recently I saw that there was a power struggle going on over the right to tap into those communications by law enforcement. It's a whole new ball game out there, and it could be that the Feds are going to put the hex on the whole operation by stifling free speech.

Unfortunately, Mr. Zimmerman's software refused to work, so we were not able to see it in action. Nevertheless, I really enjoyed his presentation.

Speaking of free speech, the entire conference was overshadowed by what had occurred between Cisco and researcher Michael Lynn earlier in the week. Cisco filed a restraining order against the management of the Black Hat Conference and Michael Lynn. Mr. Lynn had lectured on Wednesday about vulnerability in their routers that could allow hackers to shut down the Internet-literally.

Although he had already given his presentation on Wednesday, prior to the court action, Cisco pressed on to prevent him from speaking any further on their "proprietary information."

Cisco and Internet Security Systems tried to stop Mr. Lynn from speaking out, but he quit Internet Security Systems and exposed the information anyhow. He is now the subject of an FBI probe according to his attorney, Jennifer Granick.

On Wednesday Michael Lynn said "What politicians are talking about when they talk about the Digital Pearl Harbor is a network worm. That's what we could see in the future, if this isn't fixed."

The entire episode spawned yet another mini-industry, T-shirts emblazoned with "CiscoGate" were selling like hotcakes, and everybody wanted one.

Most of the hacking community praised Mr. Lynn's efforts. That's what DefCon is all about, exposing network weaknesses so that they can be fixed. If such efforts are met with Gestapo tactics it can do nothing but harm us all. Why not just get on the ball, Cisco, and fix your stuff instead of terrorizing Mr. Lynn because you didn't design your stuff properly in the first place? Just like the government, corporate America never has the time to do things right, but they always seem to find plenty of resources to make things tough on whistleblowers who are just pointing out what they should have done in the first place. Where's the logic?

Actually, Michael Lynn was doing quite well thank you, receiving a number of job offers far superior to his previous job at Internet Security Systems. And he didn't seem concerned at all with the bully tactics of Cisco.

There is much vulnerability on the Net, if it's not exposed and repaired, the only people that will know about the risks are the guys your Mom told you about...

Another interesting presentation was done by Major Malfunction, Adam Laurie of thebunker.net. He demonstrated vulnerability in the IR systems of the hotel TV's.

Apparently the hotels don't think anyone's going to have the savvy to play with such things, and because of that it opens the door to learning much about the hotel's occupants. All that's needed is a USB TV tuner and a laptop. Laurie showed that the system could be controlled at the TV, rather than by administrators at the server. And that password protection and authentication was non-existent.

Laurie said that he had used this in a number of hotels across the country. He said there were only 2 main systems and once he figured out how to work these, there's no more learning curve, I mean, every hotel uses one of these two systems. He had used this technique on several occasions, viewing restricted movies, the email of other occupants of the hotel that had accessed their email through the system, and opening electronically controlled bar cabinets. Now that's some innovation. He claims to also be able to view the billing details of any of the other occupants. This could have some major repercussions. After all, a competitor staying in the same hotel as you could read your confidential email, and make note of anything that you purchased. Gives me the willies.

Johnny Long was also there, talking about his Google hacks and some of the interesting things he had come up with by using them. He says the problem is not with Google itself, but rather that many people were not aware of the vast amount of information that the powerful search engine was able to innocently dig up.

Using information gained solely by using Google, he claims that he was able to control PBX systems, routers, web cams, web sites themselves and printer networks.

Perhaps the most entertaining remarks were those about finding out how to access people's electrical automation via Google. He claims to have been able to control lights, coffee pots, etc. and in one case even found an item entitled "electric bong." Hmm. Not sure what he did with that one.

There were also a couple of impressive record-breaking demonstrations. Flexilis gave a demonstration reading of RFID tags at distance far further than previously thought possible.

RFID is a hot topic on the minds of many. The forces promoting RFID claim that it can only reach out and touch to 20 feet (6 meters). These enterprising young fellows proved them to be wrong. They climbed on top of their hotel roof and read tags from various distances up to 69 feet (21 meters).

The government has proposed these things for usage with U.S. passports by early next year. I don't know about you but I wouldn't want to be walking around with such an ID broadcasting to whoever decided to tune in. Others have mentioned that kidnappers could use the information to pick traveling U.S. citizens out of a group. It's bad news to me no matter how you slice it.

RFID for production purposes, keeping track of cattle, inventory, etc. is fine. But when I'm carrying an "always on" transmitter that can't wait to pass along details about me, with no record of the transfer of information to me, I just don't need it.

Flexilis was able to achieve these impressive results with two long yagi antennas (one receive, one transmit) and a box of simple electronics. Hmm. Do you suppose someone might be able to duplicate this? Someone who had figured out a way to utilize people's personal information for identity theft, etc.? You bet they can and they will.

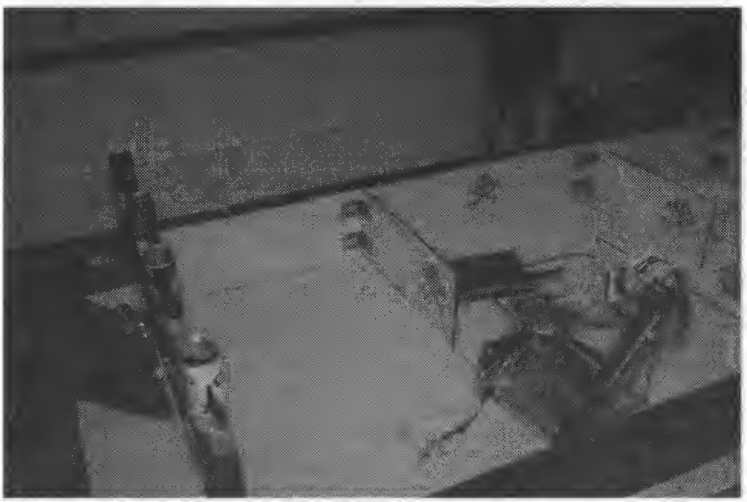
Another impressive record breaker was from a team of radio amateur friends from Xavier High School in Cincinnati, OH. who called themselves Team iFiber Redwire. They broke the record for unamplified WiFi signal range. They used two standard 802.11b WiFi cards (Z-Com 325hp). These had external antenna jacks and they hooked up large satellite dishes to those (a 10 ft. and a 12 ft.). Part of their team went to a place called Utah Hill in, of all places, Utah. That was where they sourced the connection. With this rig they were able to demonstrate a 12 ms ping time, create a SSH connection, and view a remote desktop using VNC – all at a distance of 125 miles! And get this, these 300mw WiFi cards were toned down to 30mw. Impressive indeed. So how come my stock 802.11G system has trouble reaching the next room, 50 feet away?

The world distance record for a WiFi connection was achieved by a Swedish group a couple of years ago. They established a WiFi connection to a WiFi access point tethered to a weather balloon 200 miles away. But many at DefCon pointed out that this accomplishment was much more meaningful, partly because the Swedish folks used an amplified signal. Also, this demonstration was ground-based, which has much more opportunity for the signal to be degraded on the way, due to obstructions, etc.

These results beg the question: When do we get the WiMAX? I keep hearing it's coming, and now the WiFi guys from Ohio have demonstrated fantastic things with lowly WiFi. Sigh.

The Robot Warez contest was exciting. In this competition the robot would gather up ping-pong balls and fire them at targets with some real force behind them. The team from Florida won. But it was a close match.

The other team lost because the loading operation of their robot wasn't very automated, requiring much lost time in reloading.



The target-shooting robot takes aim, leveling another mighty barrage of deadly ping-pong balls at the soda cans. Don't laugh, one fellow did get hit and it left a welt.

The Shmoo Group was demonstrating it's Bloodhound WiFi gun. They claimed that it could detect access points from miles away. AND, it was very impressive looking. I guess they felt they had to up the bar after last year's WiFi pistol.

The Lockpicking contest was a winner as well. After all, sometimes the only way to the computer is through a lock. This was the 2nd year for this contest, and it was a big hit from the prior year. There were some skilled entrants, but as the contest progressed, so did the degree of difficult hardware (locks). In the second and final round a guy with the handle Gandalf picked his lock in about 6 seconds. The battle for 2nd place then lasted over an hour, until one of the other two finalists managed to open their lock.

There were also vendors doing a swell business selling lock-picking equipment.

There was a War Driving competition. This involved teams tracking WiFi signals while driving and walking. Imagine that.

Capture the Flag at DEFCON attracts some of the best hackers in the world. Teams of hackers all try to break into a central server and each other's servers while defending their own. It's one of the best known events at DefCon.

The Scavenger Hunt required some cleverness. One of the ways in which a team could score points was in the "Creative Use of a Slinky" category. One team used a Slinky to pick a lock, I liked that. Another team used one to create one of the items on the list, nunchaku (pronounced nunchucks). They also used salami.

I was very disappointed that the DC Shoot was canceled this year. I know that CHS was not happy either.

I very much enjoyed the "Building Wardriving Hardware" workshop given by Mat Shuchman of WarDrivingWorld.com. He discussed the features and benefits of antennas, chipsets, cables, wireless cards and many other types of WiFi hardware. And then he discussed the materials to consider for making a homemade "cantenna."

The lecture on "Attacking Biometric Access Control Systems" was very informative also. Given by a fellow with the handle of Zamboni, he discussed exactly that, attacking biometric systems. He shocked many by not only explaining how to do it, but actually recommending that hackers begin targeting such systems immediately. In fact, to quote him directly he said "Attack them as you would Microsoft and Cisco." Nuff said.

Fyodor gave a great presentation on "Hacking Nmap." He described some of the things that you could do with the latest issue of nmap DC13. As with his presentation a couple of years back, this is a Do Not Miss presentation. He said that the slides from the presentation would be on the web soon, so you can still catch this material.

The badges issued at DefCon were to be worn at all times, and this rule was strictly enforced. They were very unique, made of colored Plexiglas, very thick. Presumably this was to thwart badge counterfeiting. However, at one party just before the end of the conference, the partygoers were issued forged badges that were perfect replicas in every way. Except that the colors were totally different. So much for that kind of security.

Finally there were many other lesser contests. The TCP/IP drinking game, Dunk the Hacker.

One attractive girl was walking around with a handwritten sign selling "Kisses - $1.00". I talked to her and she said that she spent everything that she had getting there (to DefCon) and now had to get cab fare home. Hmm. A little different from the usual Vegas hard luck story. She claimed to have done the same thing last year and made something like $100.

Everyone was extremely friendly. So much for the "geek" stereotype, I found that everyone was very helpful in explaining difficult concepts. No one put you down if you didn't get it the first time. Such friendly surroundings only enhanced what was a wonderful 3 day gathering. Quite a bargain at $80, learning all of the latest greatest secrets about security and the Internet, the entertainment value was worth it alone. I had a great time.

Of course, I visited Alex at the Blacklisted 411 booth. Blacklisted 411 saw fit to present us with the "Booth Babes", a few lovely ladies that seemed to keep the guys interest. They had a booth, and gave away tons of free magazines and swag (shirts, hats, stickers) and even gave out some IPODs to people that won their drawing.

One of the lovely "Booth Babes" at the Blacklisted 411 exhibit. Tons of swag was passed out by these guys.

In fact, I may be biased. But the Blacklisted 411 hats were just about the finest of the whole show. With a nice Velcro adjustable strap that was always tucked neatly out of the way. Mine said "HACK THE SYSTEM." Cool.

My favorite talks were the Phil Zimmerman encrypted VoIP and Richard Morris Sr. on the threat to ATM machines.

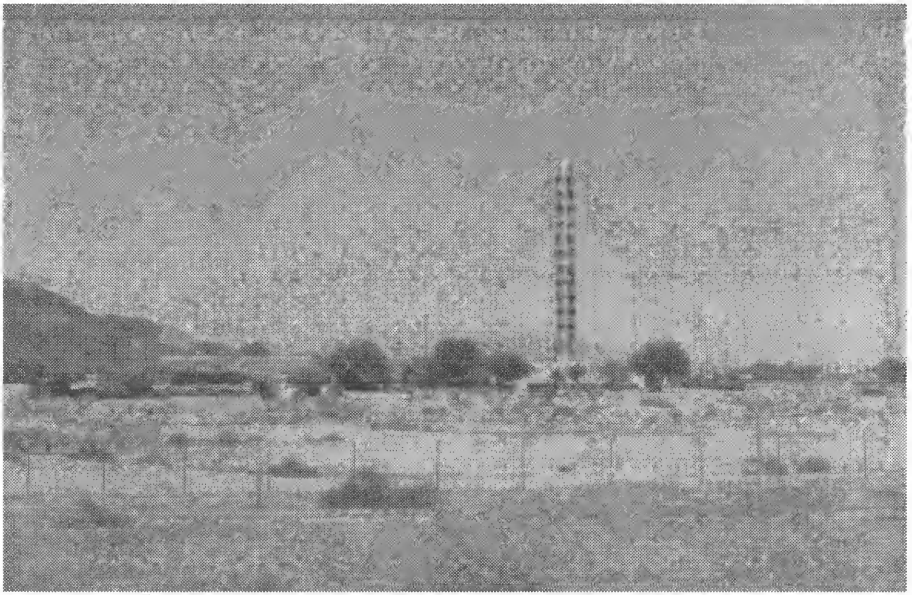
As far as the demonstrations, it's hard to beat the 125 mile unamplified WiFi by the young men from Ohio. That was really something. The RFID 69 foot read was special too; I think that Flexilis has gone a long way in spreading the awareness about the far-reaching implications of this technology. "Our goal is to raise awareness," said John Hering, one of the founders of Flexilis. Bravo.

Or the Robot Warez. That was pretty neat too. Lethal ping-pong balls.

In retrospect, I guess what I enjoyed the most was the chance to meet and hang out with some of the brightest and smartest people in the business. The rest of the year, you can stay in touch by email or whatever, but there's nothing that will ever replace being in the same room with someone who enjoys the same things that you do.

Hopefully, I'll get another opportunity to go again next year. On somebody else's dime as a reporter again. But even if I have to pay personally, I'm going! There was never a dull moment. And even when you've had enough hacking, there's always something in Las Vegas to keep you entertained. It's a win-win.

But after spending 3 days in Las Vegas, I couldn't wait to get home and check out some of the info I received. On the way home I passed "The World's Largest Thermometer" in Baker, CA. It's about a million miles from anywhere, what's that place doing there? Anyhow, one of the residents clued me in that the real name is "The World's Largest RECTAL Thermometer." I liked that better too.



World's Largest Rectal Thermometer?

WANTED

Photographs!

If you have a photo of a payphone, local telephone company vehicle or building, local cable company vehicle or building, interior of a telecomm. or other utility building, inside a manhole, inside a utility box or some other interesting item, please send them to us along with a short "memo" explaining what it is that we're looking at!

If you send a photo that we end up using in our magazine, we'll mention your name along with the photo.

The Black Market

LARGE SELECTION of items of interest to the hacker community. Surplus, stun guns, pepper spray, hobby supplies, electronics, survivalist, spyware, too much to list here. Huge selection of **FREE** ebooks, Succeed With Women, Guerilla Web Promotion, many others, some for purchase, the cream of the crop. Come check us out! www.hacksupplies.com

URBAN EXPLORATION! Phone obsessions! Pointless conversation! And a slight chance of hacking! It's Doug TV baby http://www.dougtv.org

THE WORLDWIDE WARDRIVE is an effort by security professionals and hobbyists to generate awareness of the need by individual users and companies to secure their access points. The goal of the WorldWide WarDrive (or WWWD) is to provide a statistical analysis of the many access points that are currently deployed. http://www.worldwidewardrive.org/

LOCKPICKING101.COM Open forum discussion to educate yourself and others about lock picking and lock security.

LOOKING FOR HACKERS AND PHREAKERS! We're looking for hackers and phone phreakers to work on a new community based WWW project. If you're interested and would like to know more, email keynet@spoonybard.org or visit http://spoonybard.org/keynet.html

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles will come from newspapers, magazines, online resources, and more. For more information: http://www.c4i.org/isn.html

I'M RAFFLING my original APPLE-1 computer I have no use for it anymore so I'm giving any one who wants a chance on owning a piece of history all I ask is for a one paragraph letter telling me why you would want my computer, and $2.00 cash or money order to: MY RAFFEL, 567 W. channel Isl. Blvd., Port Hueneme CA, 91341 suite 416

HACKERSHOMEPAGE.COM - Your source for Keyboard Loggers, Gambling Devices, Magnetic Stripe Reader/Writers, Vending Machine Defeaters, Satellite TV Equipment, Lockpicks, etc...(407)650-2830

HACKER STICKERS Geeks, Coders and Hackers get your stickers, shirts, hardware and caffeine from www.hackerstickers.com

CELLULAR PROGRAMMING CABLES: For Motorola Flip Series $100, 8000/Brick Series $150, Mobile/Bag: $100 (includes handset jack, the only way to program Series 1). Panasonic and Mitsubishi Cables $100. All cables are high quality, professionally assembled and guaranteed. Guide to Cellular Programming, everything you ever wanted to know, correct wiring diagrams, troubleshooting, etc.: $45. Other accessories and programming software available. Inquiries to: (714)643-8426, orders only to: (800)457-4556. C.G.C.

SCANNER MODIFICATION HANDBOOK. Big! 160 pages! More than 20 performance enhancements for PRO-2004 and PRO-2005. Restore cellular, increase scanning speed, add 6,400 memory channels, etc. Step by step instructions, photos, diagrams. Only $17.95, + $3.50 hipping ($4.50 Canada). (NYS residents add $1.38 tax.) CRB research, Box 56BL, Commack, NY 11725. Visa/MC welcome. (516) 543-9169.

HIGH-TECH security/survival books/manuals: Computers, Internet, Phones, Energy, Physical Survival, Financial, Law, Medical/Radionics, Mind Control, Weird/Paranormal. Free Online Catalog at: Consumertronics.net (PO 23097, ABQ, NM 87192), or $3 hardcopy (USA/Canada, $7 foreign). See display.

SIX DIGIT LED CLOCKS (with seconds); AC powered, highly accurate. Several models. Free catalog! Whiterock Products, 309 South Brookshire, Ventura, CA 93003. (805) 339-0702.-9169.

CELL PHONE cloning for the guy who has (two of) everything. Must have current service contract. For more info, call Keith (512)259-4770. 6426, Yuma, AZ 85366-6426.

BUILD A RADAR JAMMER out of your old radar detector. No electronic knowledge needed. Only $9.95 + $2.50 S&H Call 24fr. for easy step-by-step plans. 1-800-295-0953 Visa/MC/Dis.

ALL YOUR 802.11B ARE BELONG TO US Unlike any other database system that exists since or during the period of "the collective" (2002), none other has given a return of the entire collective back to the submitter. The collective is not a mapping database system. It is a mechanism to exchange data in a cumulative fashion for such interested parties through anonymous assimilation. http://www.allyour80211barebelongtous.org/

SCIENTIFIC ATLANTA 8580 $225, 8570 $250, 8550 $150, 8500 $120. Will program your 8550, 8500 EAROMS for $7.50. Cable security key gets past collars $25. Add $5 shipping. No TX sales. Send money order to: K. Perry, PO Box 816, Leander, TX 78646-0816. Phone: (512)259-4770.

HEAR NON-COMMERCIAL SATELLITE RADIO programs right in your area without the use of a dish or any other expensive receiving equipment. Thousands of these programs are operating today across America. Programs may include talks shows, weather, sport events, news feeds, financial reports, music programs and data ports. This technology is received through a high tech. SCSRT1 card. Find out today what you have been missing! (800) 944-0630. Credit card orders accepted.

USED CELLULAR HANDHELDS: Panasonic EB3500 portables, includes a battery (but no charger) forty number alpha memory, good working order, available as an extension to your existing line for $279, or as is for $129. Orders only: (800)457-4556, Inquiries to: (714)643-8426. C.G.C.

HOME AUTOMATION. Become a dealer in this fast growing field. Free information. (800)838-4051.

TIRED OF SA TEST KITS with marginal or inconsistent performance? 21st Century Electronics and Repair guarantees peak performance with 40-pin processor kits. New, more flexible program with additional features puts others to shame. Price $49 each or 5 for $233. 1st time offered. (404)448-1396

FEDERAL FREQUENCY DIRECTORY! Kneitel's "Top Secret" registry of government frequencies, New 8th edition. 268 pages! FBI, DEA, Customs, Secret Service, BATF, Immigration, Border Patrol, IRS, FCC, State Dept., Treasury, CIA, etc. & surveillance, bugs, bumper beepers, worldwide US military, 225 to 400 Mhz UHF aero band, Canadian listings, & more! Ultimate "insider's" directory! Standard reference of law enforcement, news media, private security, communications industry & scanner owners. $21.95 + $4.00 shipping ($5.00 to Canada). NY State residents add $2.21 tax. CRB Research Books, Box 56BL, Commack, NY 11725. Visa/MC welcome. Phone orders (516) 543-9169 weekdays (except Wednesday) 10 to 2 Eastern.

TV CABLE/SATELLITE ("GRAY" MARKET) DESCRAMBLER EXPOSE, 160pp, illustrated, with vendor lists for chips, parts. Law, countermeasures, much more! $23.95 + $3 S/H. Check/MO. INDEX, 3368 Governor Dr., Ste. 273, San Diego, CA 92122. Credit cards only: (800) 546-6707. Free catalog of "insider" books on scanners, cellular, credit, eavesdropping, much more.

TOP SECRET SPY DEVICES Home of the Worlds' Smallest Digital Voice Recorders and Spy Cameras. We stock many items including: Transmitters, Bug Detectors, Audio Jammers, Telephone Recorders, Lock Picks, Voice Changers, Keystroke Loggers. www.spydevicecentral.com (305)418-7510

HACKERS '95 THE VIDEO by Phon-E & R.F. Bums: See what you missed at Defcon III and Summercon 95! Plus, our trip to Area 51 and coverage of the "CyberSnare" Secret Service BUSTS. Elec Cntr Measures, HERF, crypto, and more! Interviews with Eric BlookAxe, Emmanuel, and others. VHS 90 min. Only $25 - distributed by Custom Video 908-842-6378.

EUROZINES AND OTHER CULTURAL HACKER ZINES! A one-stop, cutting-edge mail-order source for over 1,000 titles. Beautifully illustrated 128-page catalog includes: alternative/fringe science, conspiracy, Forteana, sexuality, computer hacking, UFOs, and much more. Send $3.00 to Xines, Box 26LB, 1226-A Calle de Comercio, Santa Fe, NM 87505.

CELLULAR RESTORATION on your 800 Mhz scanner performed expertly for $40 including return shipping. Guaranteed. Offer expires soon. Keith Perry, 607 Osage Dr., PO Box 816, Leander, TX 78641. (512) 259-4770.

6.500 MHZ CRYSTALS $4 a piece, 50 for $115, 100 for $200. Add $3.00 for shipping. Send checks to C. Wilson, P. O. Box 54348 Philadelphia, PA 19105-4348

SPECIAL SALE amd 2400+ system with 256mb ram, 40gig hdd, 64meg int video w/agp slot and extremely portable case w/handle $450.00 + shipping handling. for details send email to xteraco@yahoo.com w/ subject special sale??

COIN-OP VIDEO ARCADE GAMES. Parts, boards, and empty cabinets available for your projects. Cabinets available for $75. C.J. Stafford, (301)419-3189.

THE BLACK BAG TRIVIA QUIZ: On MSDOS disk. Interactive Q&A on bugging, wiretapping, locks, alarms, weapons and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining and VERY educational. Includes catalogs of selected (no junk) shareware and restricted books. Send $1.00 for S.25 disk, $1.50 for 3.5, plus two stamps, to: MENTOR PUBLICATIONS, Box 1549-W, Asbury Park NJ 07712

ANARCHY ONLINE A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers and phone phreaks. Scheduled hacker chat meetings. Encrypted E-mail/file exchange. WWW: hhtp://anarchy-online.com Telnet: anarchy-online.com Modem: 214-289-8328

WAR DRIVING IS NOT A CRIME The benign act of locating and logging wireless access points while in motion - Wardriving is NOT a crime, being stupid should be. http://www.wardrivingisnotacrime.com/

HACK THE PLANET A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3.00 check or money order payable to CASH. Hand-scanned 99XX exchanges in 516 AC. Included may be data kit modem numbers, WFA/FA, SSCU, TSAC(SCC), CO#'s, etc. Send $2.00 check or money order payable to CASH and specify exchange. "MCI-Style" Phone Patrol hats are now available! Just $18 check or money order payable to CASH. 2447 5th Ave, East Meadow, NY 11554.

ATTENTION HACKERS & PHREAKERS. For a catalog of plans, kits & assembled electronic "TOOLS" including the RED BOX, RADAR JAMMER, SURVEILLANCE, COUNTER SURVEILLANCE, CABLE DESCRAMBLERS & many other HARD-TO-FIND equipment at LOW PRICES. Send $1.00 to M. Smith-02, P.O. Box 371, Cedar Grove, NJ 07009

PRIVACY ACT AND SOCIAL SECURITY NUMBER LIMITATIONS, How anyone can win $10K fine for this simple violation of your rights. Open a bank account without a SSN $5 plus 3 F/C stamps. Obtain a major credit card without a SSN (making it impossible for a bank or any institution to check your credit history or records) $25 plus 5 F/C stamps. For info send $1 and LSASE to: Know Your Rights, c/o R. Owens, 1403 Sherwood Dr., Bowling Green, KY 42103. NO CHECKS PLEASE. M/O or FRN's only.

VOICE CHANGING ACCESSORY. Digital voice changing: male to female, female to male, adult to child, child to adult. Use with any modular phone. 16 levels of voice masking. Connects between handset and phone. STOP THOSE ANNOYING TELEPHONE CALLS! Sound older and tougher when you want to. Not a kit. Fully assembled. Use with single or multi-line phones. 30-day refund policy. Ask for free catalog of our products. VISA/MC ok. Xandi Electronics. 1270 E. Broadway, Tempe AZ 85282-5140. Toll Free order line: (800)336-7389. Technical Support: (602) 894-0992

MAGENCODERS.COM Manufacturer of the World's Smallest Portable Magnetic Card Reader & Point of Sale Data Loggers. We also have Magnetic Stripe Reader/Writers, Smart Card Loaders & Copiers, etc... (407)540-9470

UNDETECTABLE VIRUSES. Full source for five viruses which can automatically knock down DOS & windows (3.1) operating systems at the victim's command. Easily loaded, recurrently destructive and undetectable via all virus detection and cleaning programs with which I am familiar. Well-tested, relatively simple and designed with stealth and victim behavior in mind. Well-written documentation and live antidote programs are included. Priced for sharing, not for making a ridiculous profit. $10.00 (complete) on six 1.44MB, 3.5" floppy discs. Money orders and checks accepted. No live viruses provided! Do NOT ask. Satisfaction guaranteed or you have a bad attitude! The Omega Man. 8102 Furness Cove, Austin, TX 78753

NO SOUND ON PREMIUM CHANNELS? It will happen sooner or later on your Jerrold DPBB-7 Impulse. Ask Manhatten! Soundboard brings the sound back. Best sound fix on the market. Easy to install soundboard $24.95. Easy to build soundboard schematic, parts list and common chip number $34.95. Send us your unit and we will install the soundboard for $59.95. SOUNDMAN, 132 North Jardin St., Shenandoah, PA 17976. (717) 462-1134.

SINGLE DUPLICATION OF CD-ROMS Send your CD and $25 and you will receive your CD and an exact copy. Want more than one copy? Send a additional $15 for each duplicate. Make checks or money orders Payable to/Mail to: Knoggin, 582 Merket Street Suite 616, San Francisco, CA 94114

FIND PIRATE SOFTWARE Learn how to find pirate software on the Internet. Get thousands of dollar's worth of programs for free such as Office97 and more games than you can play. Complete guide includes background, tools, techniques, locations, and shell scripts that will find software for you! Send $5.00 money order or CASH (no checks) to The Knoggin Group, P.O. Box 420943, San Fransisco, CA 94121-0943, USA.

CB RADIO HACKERS GUIDE! New! Big 150 pages; pictorials, diagrams, text. Peaking, tweaking and modifying 200 AM and SSB CB radios. Improved performance, extra capabilities! Which screws to turn, which wires to cut, what components to add: Cobra, Courier, GE, Midland, Realistic, SBE, Sears, Uniden/President. $18.95 + $4 S&H ($5 Canada.) NY State residents add $1.96 tax. CRB research, Box 56BL, Commack, NY 11725. Visa/MC accepted. Phone order M-Tu-Th-F, 10 to 2 Eastern time. (516) 543-9169.

NULL MODEMS - Download laptop: or upload to your pc the easy way! w/ direct connect, or (DOS 6.1) Customized setup, no bulky adapters, MAC or IBM compatibles. Send $18.95 for 6ft cable, specify 25 or 9db ends, custom ok. Instructions included. P.O. Box 431 Pleasanton, CA 94566 (510)485-1589

DON'T BUY A MODIFIED CABLE CONVERTER! I'll show you what to do. Where to get parts, everything. Call 24hr.. 1-800-295-0953 Only $9.95 + $2.20 S&H Visa/MC/Dis.

A TO Z OF CELLULAR PROGRAMMING. Programming instructions on over 300 phones in a software database. Also back door and test mode access instructions for all the popular models; manufacturer's contacts, system select, lock/unlock info. Just $59.95. Orders only: (800)457-4556, inquiries: (714)643-8426. C.G.C.

GAMBLING MACHINE JACKPOTTERS We offer a complete range of gambling products designed to cheat gambling machines as well as other games. Our products are designed to demonstrate to gambling machine owners the vulnerabilities of their machines. Our product line consists of Gambling Machine Jackpotters, Emptiers, Credit Adding Devices, Bill Acceptor Defeats and Black Jack Card Counting Devices. Please visit www.jackpotters.com

KEYSTROKEGRABBERS.COM Manufacturer of discreet keyboard logging hardware. Our devices capture ALL keystrokes on a computer including user name and password. PARENTS---Monitor your child's internet, e-mail, instant messaging and chat room activity. EMPLOYERS---Monitor employee computer usage compliance. Employees will spend less time browsing the internet and sending e-mails if they are being monitored. EXECUTIVES & SYSTEM ADMINS---detect any unauthorized access of your PC. If someone uses your computer after hours, you will know. (305)418-7510

HACKING, PHREAKING, computer security and education on the First Tuesday of every month in the Detroit area. Meeting is at 7pm at Xehdo's cafe in Ferndale. Bring your open mind and positive attitude.

A SHOW ON URBAN Exploration. WhiteSword TV http://WhiteSword.tk

I WANT TO OFFER my playstation 2 game burning service. Any game that you would like for a back-up or just for fun. Or maybe that Japanese game that just won't be out in the United states for a few months.. I have bundles that you can choose from if you want handfulls depending how much you order. the games are $25 each !PLEASE NOTE THAT YOUR PLAYSTATION 2 NEEDS TO BE MODDED I ALSO HAVE THAT SERVICE BUT YOU CAN ALSO GOOGLE SEARCH FOR PREMODDED SYSTEMS TO BUY. EMAIL IF YOU HAVE ANY QUESTIONS AT ALL.

ACCUSED OF A COMPUTER RELATED CRIMINAL OFFENSE IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in the defense of alleged cybercriminals, including but not limited to, hackers, crackers, and phreaks. Not a former prosecutor seeking to convince defendants to plead guilty, but an idealistic constitutional and criminal defense attorney who helped secure a total dismissal of all charges in Los Angeles Superior Court for Kevin Mitnick, who was falsely charged with committing computer-related felonies in a case with $1 million bail. Please contact Omar Figueroa, Esq., at (415) 986-5591, at omar@aya.yale.edu or omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Complimentary case consultation for Blacklisted 411 readers. (Also specializing in medical marijuana and cannabis cultivation cases.) All consultations are strictly confidential and protected by the attorney-client privilege.

I-HACKED.COM is a hardware hacking based website and it currently looking for articles! Membership is limited to contributing members, so come and share your knowledge with other hackers around the world. Topics we are currently looking for include: DVD "Dual-Layer" Firmware hacks, CD-RW / DVD+/- Speed Hacks, Video Card Hacks, Motherboard Hacks, IDE Card / Raid Hacks, Xbox Hacks, Playstation Hacks, cell phone tricks, or anything else you might have. Check us out @ http://www.i-hacked.com

SUPPORT OUR HACKER COMMUNITY! I happened upon this site looking for an image hosting service and thought I'd share it with the rest of the community. It's called Smugmug and you can find it at www.smugmug.com. Not only do they have a high quality service going on, but they also feel about hacking as we do. Check out what they say about hacks on their website! I've been using their service for a while now, and I can honestly say that what they pay attention to the little details. By far the best photo site out there! Because they understand what hacking really is, they know what they're talking about. Why does this matter? Well, they too are probably hackers and we all know that hackers can put together something great when they put their minds into it. Store unlimited photos starting at only $29.95/year....that's right a year! That's a great bargain! There is a free 7 day trial offer, and if you use the code NTQ0He0Ou527E you'll get a $5 discount.

BLACKLISTED MEETINGS will begin in Greece as the new year arrives, They will be held every 3rd saturday of the month and they will begin at 7pm. Meeting point will be the centre of Athens at the metro station Panepistimio by the fountains. Also check the webpage www.blacklisted411.gr.

A+ CERTIFIED TECHNICIAN offering cheap repairs in Louisville Area. Will make house calls or take home with me. I do everything from virus and spyware removal to networking. Send an email to alanb6100@gmail.com with your name and phone number as well as a description of the problem. Also I have Gmail invites available for a reasonable price. Louisville area only unless you want to Western Union me some money! Thanks!

THE NEWEST DEVICE on the market it the new Sony PSP. Already there are numerous hacks out to make it do your bidding, whether it be surfing the net, or using memory sticks to watch movies the sony psp is powerful. These are a hot commodity. Get them before they are gone.
Get them from Phreepsps.com

HI, MY NAME IS RICK. Me and my friend Rob where looking for a low cost rackmount server one day to use for a web and mail server that we could have racked at a local datacenter, Not finding anything real cheap we decided to start our own company building fast cheap servers for you also. www.cheap1u.com was born. Mention this ad and get 10% off any server order. Also since I am the owner, if you mention this ad buy 10 servers and I will throw in the 10th server for free! Thats right even our $399 AMD powerhouse!

SELLING USED HIRSCH SCRAMBLEPADS that retail new for around 500$ for your best offer! They are for very high security places, every time you press the START button on the keypad it randomizes the digits so that any onlookers cannot find a pattern in the digits you press. Also, you cannot see the numbers from the side, so for anyone to see your code they would have to be directly behind you. Email me for more information. guiltyspark414@netscape.net

TUNE IN TO CYBER LINE RADIO on the internet, on the USA Radio network. We can be heard Saturday Evenings 9:00 pm to 12:00 am (Central). Heard Exclusively On The USA Radio Network & Via The Internet! We discuss Technology, Space, Hacking, Linux and more. For more details meet us at www.cyber-line.com.

CELLULAR EXTENSIONS, SEND US YOUR PHONE or buy a new or used phone from us! Proof of line ownership required. We have phones from $129. Call for a list of available models, we program many different brands including all Motorola, same day service. Orders only: (800) 457-4556, inquiries to: (714)643-8426. C.G.C.

TRUE TAMPER-PROOF Security Screw Removal Bits. The super torx kit includes: T-10, T-15, T-20 & T-25. Complete set for $19.60. TOCOM 5503 bit $8.95. TOCOM 5507 bit $19.95. Zenith PM/PZ-1 bit $10.95. Jerrold Starcom bit $19.95. Pioneer (oval) bit $23.95. Oak Sigma (oval) bit $23.95. Security Screws available. Tamper-Bit Supply Co. (310)866-7125.

WANTED: FEATURE FILM JUNKIE who can access up-to-date FAX numbers for hot agents and/or producers & directors. My objective: to bring to their attention my action-thriller script. Can pay by the hour. (909)275-9101

DO YOU WANT MORE underground information? Are you ready to go to a whole new level of knowledge? Then you need to check out "Binary Revolution" magazine.
 is a printed hacking magazine put out by the DDP that covers hacking, phreaking, and other assorted topics from the computer underground. For more information on the magazine, forums, HackRadio, HackTV, or any of our other numerous projects, come to www.binrev.com and join the revolution. "THE REVOLUTION WILL BE DIGITIZED."

NEW HACKING WEBSITE: Hackit.org has hacking guides, forums,tools and more. Much more. Check it out!

Marketplace classified advertising is currently FREE to anyone. It's a first come, first served offer, limited only by space constraints within each issue. If you'd like an ad placed within Blacklisted! 411, you should send it in as soon as possible. We accept both commercial as well as personal ads. We may decide not to publish any ads which are inappropriate or have no connection with the hacker community.

CONTACT US AT: www.blacklisted411.net

WWW.BLACKLISTED411.NET

MONTHLY MEETINGS

Interested in meeting up with some of the Blacklisted! 411 readers? We will list all hacker meeting information that is provided to us. We will list "Blacklisted! 411" only meetings as well as "independent" meetings open to all.

Califomia

(949 Area Code) - Irvine

iHop - By Airport (Upstairs Room), 18542 MacArthur, Irvine, CA. 92714 - Meeting is not Blacklisted! 411 specific. The meeting date may change from month to month. For specifics, check here: www.irvineunderground.org
Hosted by: Freaky

New Mexico

(505 Area Code) - Albuquerque

Winrock Mall - Louisiana at I40, food court, east side doors under the security camera dome.
First Friday of the month, 5:30pm - 9:00pm
Hosted by: Mr. Menning

Wyoming

(307 Area Code) - Rock Springs/Green River

White Mountain Mall—Sage Creek Bagels. The last Friday or every month from 6:30pm until 9:30pm.
Hosted by: Phreaky

Florida

(407 Area Code) - Orlando

The computer room in the Grand Reserve Apts. at Maitland Park
Last Friday of the month, 12:00pm - 1:30pm
Hosted by: Whisper

Texas

(713 Area Code) - Houston

In front of Rocfish on Westheimer/Kirkwood. Last Sunday of every month, 7:00pm till close.
Hosted by: MuertoChongo

Colorado

(719 Area Code) - Colorado Springs

DC719 - Hack the Rockies. Meetings held on the 3rd Sat. of every month. 8pm-11pm @ Xtreme Online, 3924 Palmer Park BLVD
Hosted by: DC719 POC: h3adrush

(303 Area Code) - Centennial

We meet the first Friday and third of every month at 5:00pm at the Borders café on Parker in Arapahoe Crossings.
Hosted by: Ringo

Georgia

(678/770/404 Area Codes) - Duluth

Meetings are the first and third Tuesday of every month, in the cafe of Frys Electronics. They start at 6:30 until we get kicked out, and then continue elsewhere. Visit our site at www.HackDuluth.org and sign up on the forums to receive emails about the group.
Hosted by: P(?)NYB(?)Y

(678/770/404 Area Codes) - Snellville

Borders at 1929 Scenic Highway, first Saturday of every month. 8:00PM
Hosted by: iamsam (comingtoleave@gmail.com)

Mexico

(666 Area Code) - Tijuana, B.C.

Café Internet, Calle 12, Felix M. Gomez #844, Col. Libertad. In back room by payphone. First Friday of the month, 5:00pm to 8:00pm
Hosted by: Tom

YOUR MEETING HERE

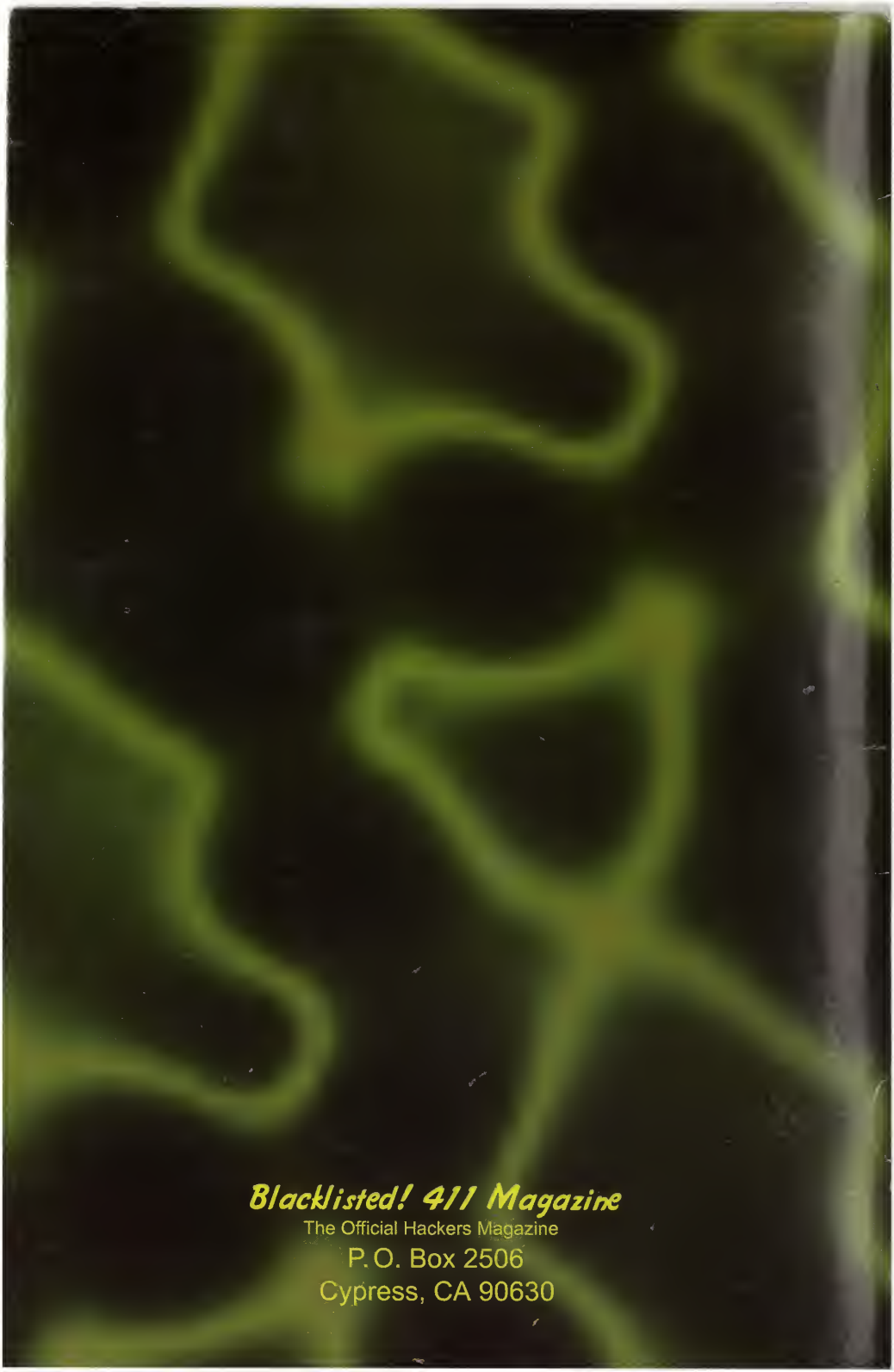
Start up your own meeting! Contact us right away!!

BLACKLISTED 411 WANTS YOUR ARTWORK

Are you an artist? Do you like Blacklisted! 411? Do you hate Blacklisted! 411? Well, if you're looking for work, it doesn't matter if you like us or not, does it? If you'd like to show off some of your talent, why not send us some samples on PAPER or send us a disk with your sample artwork. We'd be happy to show off your work, give you a free subscription or make some other arrangement if you'd like. If you're interested, take a look through the magazine and make note of the existing artwork. Think about it and try to come up with something completely original which coincides with the general theme of the magazine. A few ideas to consider: Pirates, Skull & Crossbones, Einstein, Computers, Electronics, Phones, Cable TV, Satellite TV, Radio, etc.

Here's who you send your artwork to:
Blacklisted! 411 ARTWORK
P.O. Box 2506, Cypress, CA 90630

***We WANT to hear from YOU....*don't delay - just send us what you have. We prefer freehand artwork on PAPER, but will accept in high resolution (if at all possible) computer graphics formats: TIF, TGA, JPG, GIF, PSD, PCX and most other popular image formats.**


Blacklisted! 411 Magazine
The Official Hackers Magazine
P.O. Box 2506
Cypress, CA 90630